

普通高等教育"十一五"国家级规划教材

高 等 院 校 信 息 安 全 专 业 系 列 教 材

教育部高等学校信息安全类专业教学指导委员会
中 国 计 算 机 学 会 教 育 专 业 委 员 会
共同指导

顾问委员会主任：沈昌祥 编委会主任：肖国镇

信息安全体系结构

冯登国 孙锐 张阳 编著
蔡吉人 审

http://www.tup.com.cn

Information Security

根据教育部高等学校信息安全类专业教学指导委员会制订的《信息安全专业指导性专业规范》组织编写

清华大学出版社

普通高等教育"十一五"国家级规划教材
高等院校信息安全专业系列教材

信息安全体系结构

冯登国　孙　锐　张　阳　编著

清华大学出版社
北　京

内 容 简 介

本书对信息安全涉及的各个层面进行了梳理和论证，并讨论了与安全技术和产品相关的内容，充分反映了信息安全领域的最新研究进展和发展趋势。本书主要从信息安全体系结构规划与设计、信息安全技术支撑、信息安全产品、信息安全标准、信息安全管理、人员能力成熟度模型以及信息安全应用案例等方面系统地论述了如何解决信息技术应用所带来的信息安全问题。本书也对信息安全体系结构的概念进行了详细分析和论述，并对构建信息安全体系结构的关键三要素(人、技术和管理)之间的关系进行了详细阐述。本书的特点是系统性强、内容覆盖面广、体系化程度高。

本书可作为计算机、通信、信息安全、密码学等专业的本科生和研究生的教材，也可供从事相关专业的教学、科研和工程技术人员参考。

图书在版编目（CIP）数据

信息安全体系结构/冯登国，孙锐，张阳编著. —北京：清华大学出版社，2008.9
(高等院校信息安全专业系列教材)
ISBN 978-7-302-17072-3

Ⅰ. 信…　Ⅱ. ①冯… ②孙… ③张…　Ⅲ. 信息系统－安全技术－高等学校－教材
Ⅳ. TP309

中国版本图书馆 CIP 数据核字(2008)第 021494 号

责任编辑：张　民　顾　冰
责任校对：李建庄
责任印制：李红英

出版发行：清华大学出版社　　**地　　址**：北京清华大学学研大厦 A 座
http://www.tup.com.cn　　**邮　　编**：100084
社　总　机：010-62770175　　**邮　　购**：010-62786544
投稿与读者服务：010-62776969，c-service@tup.tsinghua.edu.cn
质　量　反　馈：010-62772015，zhiliang@tup.tsinghua.edu.cn
印 刷 者：北京密云胶印厂
装 订 者：北京市密云县京文制本装订厂
经　　销：全国新华书店
开　　本：185×230　**印　张**：15　**字　数**：304 千字
版　　次：2008 年 9 月第 1 版　**印　次**：2008 年 9 月第 1 次印刷
印　　数：1～5000
定　　价：23.00 元

本书如存在文字不清、漏印、缺页、倒页、脱页等印装质量问题，请与清华大学出版社出版部联系调换。联系电话：010-62770177 转 3103　　产品编号：024968-01

高等院校信息安全专业系列教材

编审委员会

出版说明

21世纪是信息时代，信息已成为社会发展的重要战略资源，社会的信息化已成为当今世界发展的潮流和核心，而信息安全在信息社会中将扮演极为重要的角色，它会直接关系到国家安全、企业经营和人们的日常生活。随着信息安全产业的快速发展，全球对信息安全人才的需求量不断增加，但我国目前信息安全人才极度匮乏，远远不能满足金融、商业、公安、军事和政府等部门的需求。要解决供需矛盾，必须加快信息安全人才的培养，以满足社会对信息安全人才的需求。为此，教育部继2001年批准在武汉大学开设信息安全本科专业之后，又批准了多所高等院校设立信息安全本科专业，而且许多高校和科研院所已设立了信息安全方向的具有硕士和博士学位授予权的学科点。

信息安全是计算机、通信、物理、数学等领域的交叉学科，对于这一新兴学科的培养模式和课程设置，各高校普遍缺乏经验，因此中国计算机学会教育专业委员会和清华大学出版社联合主办了"信息安全专业教育教学研讨会"等一系列研讨活动，并成立了"高等院校信息安全专业系列教材"编审委员会，由我国信息安全领域著名专家肖国镇教授担任编委会主任，共同指导"高等院校信息安全专业系列教材"的编写工作。编委会本着研究先行的指导原则，认真研讨国内外高等院校信息安全专业的教学体系和课程设置，进行了大量前瞻性的研究工作，而且这种研究工作将随着我国信息安全专业的发展不断深入。经过编委会全体委员及相关专家的推荐和审定，确定了本丛书首批教材的作者，这些作者绝大多数都是既在本专业领域有深厚的学术造诣、又在教学第一线有丰富的教学经验的学者、专家。

本系列教材是我国第一套专门针对信息安全专业的教材，其特点是：

① 体系完整、结构合理、内容先进。

② 适应面广：能够满足信息安全、计算机、通信工程等相关专业对信息安全领域课程的教材要求。

③ 立体配套：除主教材外，还配有多媒体电子教案、习题与实验指导等。

④ 版本更新及时,紧跟科学技术的新发展。

为了保证出版质量,我们坚持宁缺毋滥的原则,成熟一本,出版一本,并保持不断更新,力求将我国信息安全领域教育、科研的最新成果和成熟经验反映到教材中来。在全力做好本版教材,满足学生用书的基础上,还经由专家的推荐和审定,遴选了一批国外信息安全领域优秀的教材加入到本系列教材中,以进一步满足大家对外版书的需求。热切期望广大教师和科研工作者加入我们的队伍,同时也欢迎广大读者对本系列教材提出宝贵意见,以便我们对本系列教材的组织、编写与出版工作不断改进,为我国信息安全专业的教材建设与人才培养做出更大的贡献。

“高等院校信息安全专业系列教材”已于2006年初正式列入普通高等教育“十一五”国家级教材规划(见教高[2006]9号文件《教育部关于印发普通高等教育“十一五”国家级教材规划选题的通知》)。我们会严把出版环节,保证规划教材的编校和印刷质量,按时完成出版任务。

2007年6月,教育部高等学校信息安全类专业教学指导委员会成立大会暨第一次会议在北京胜利召开。本次会议由教育部高等学校信息安全类专业教学指导委员会主任单位北京工业大学和北京电子科技学院主办,清华大学出版社协办。教育部高等学校信息安全类专业教学指导委员会的成立对我国信息安全专业的发展将起到重要的指导和推动作用。“高等院校信息安全专业系列教材”将在教育部高等学校信息安全类专业教学指导委员会的组织和指导下,进一步体现科学性、系统性和新颖性,及时反映教学改革和课程建设的新成果,并随着我国信息安全学科的发展不断修订和完善。

我们的 E-mail 地址是:jsjjc_zhangy@126.com;联系人:张玥。

清华大学出版社

本书序

21世纪，人类社会已进入信息时代。信息时代的重要特征是信息的获取、传输、处理等的高速发展。伴随信息化的发展，信息安全作用更加突出，成为全球关注的热点问题。为培养高层次信息安全人才，我国的一些高等院校设置了信息安全专业，并出版了或准备出版一系列信息安全教材。冯登国教授等编著的《信息安全体系结构》是高等院校信息安全专业规划教材之一。这是一本具有系统性、先进性和实用性等鲜明特点的教材。

(1) 系统性。信息安全的发展，人们已认识到它不仅是安全技术和产品的问题，而是一个涉及信息安全策略、整体架构、完整流程以及涵盖技术、产品、人员、过程、管理等诸多因素的复杂系统。本书从信息安全整体性出发，系统论述了信息安全的体系结构规划和设计、技术支撑、产品、标准、管理、人员等各个方面以及它们之间的关联，使读者能从更高的层次上去领会信息安全问题。

(2) 先进性。信息领域的对抗是一个永恒的命题，信息安全是一个不断发展的过程，它不会永远停留在一个水平上。研究信息安全问题不仅要能满足当前的需求，而且要求在信息安全问题迅速变化中及时适应新的要求。该书在每个部分不仅系统介绍了当前的发展状况，而且分析了它们的发展趋势，这对启发读者的思考是十分重要的。

(3) 实用性。理论联系实际是学习的一条重要原则。本书为帮助读者全面了解信息安全的应用状况，较为系统、完整地介绍了国内外信息安全相关的技术标准、管理标准和法律法规，介绍了国外的人员能力成熟度模型，还提供了若干信息安全应用案例，内容丰富，可读性强。

以上这些特点，反映了《信息安全体系结构》是一本很好的信息安全教材，相信它的出版定会引起读者的广泛兴趣。

蔡吉人
中国工程院院士

前 言

21世纪以来，随着信息技术的不断革新和广泛应用，人类社会已经步入真正的信息时代。信息技术使我们的工作更为便捷，生活更加舒适，获取信息的途径空前地增多。然而，我们不得不关注我们现在究竟生活在一个什么样的信息社会中？我们每天接触的形式多样、功能或简单或复杂的信息系统与信息网络是否具备令人满意的安全性和可靠性？是否能够及时为我们提供正常的服务？我们对这些网络与信息系统产生如此高度的依赖性，是否会在未来的某个时刻使我们的生活陷入困境？是否会像某些科幻片里讲述的那样，人类费尽心血不断尝试和改进的技术，对人类的发展而言也会带来无法控制的灾难？

不断地有来自世界各地的报道，表明这种依赖的确面临风险。北美大断电，海底电缆故障，航空系统瘫痪，计算机病毒泛滥，数以万计的信用卡账户信息被盗……即使在中国，近些年来类似的事件也层出不穷，危害明显增大。几十年前，信息安全研究与应用主要局限于军队和某些特殊需要。那时，很少有人会预料到，今天会有那么多种类的信息安全产品"飞入"到寻常百姓家。

那么，面对这种变化，面对这些事件，面对这些网络和信息系统，人们在反思：究竟应该如何设计、建设它们？如何对它们自身及其用户进行必要的管理？如何让我们精心研究、设计和开发的技术与产品帮助我们更方便、快捷地工作，更舒心、惬意地生活？

本书试图从体系结构规划与设计、相关技术与产品的设计和应用等方面回答这个问题。此外，鉴于信息安全管理的重要性日益显著，书中也覆盖了与之相关的研究内容，尤其是有关风险评估、等级保护、信息安全管理体系建设等方面的内容。

19世纪英国著名的哲学家、社会学家和教育学家赫·斯宾塞说过："科学是系统化了的知识"。本书在写作过程中，也一直希望能够对信息安全体系结构所涉及的各方面内容进行梳理，尤其是涉及技术与产品的内容。然

而，鉴于信息安全研究不断深入、技术挑战快速出现，以及相关产业的迅速跟进，我们只能力所能及地挑选现阶段相对成熟、具有代表性的内容进行介绍。书中内容没有涉及一些新技术、新产品，例如，反垃圾邮件技术与产品、反间谍软件技术与产品、IT 审计技术与产品(服务)，以及其他许多集成有信息安全功能的技术与产品(例如，带有 SSL 安全通信功能的安全负载均衡设备)。

本书多次作为中国科学院研究生院开设的研究生课程“信息安全体系结构”的授课教材加以使用。选修该课程的研究生们提出了许多宝贵意见，尤其是李立、马强、宋翊麟、张辰、黄非、薄立兴、杨清峰、周芃、张铁赢、卢山、陈波、韩钰、崔兴华、周志勇、初晓博、李昊、魏冰、吴微微、黄亮、王雷、孙彬、敬成、付允等，部分内容借鉴了他们的作业报告，在此表示衷心的感谢，这些教学实践对本书的形成具有十分重要的意义。

爱因斯坦有句名言，“学校的目标始终应当是：青年人在离开学校时，是作为一个和谐的人，而不是作为一个专家”。我们真心希望，这些研究生们，以及认真阅读这本书的所有读者，都能够在成为一个和谐的人的基础上，对信息安全体系结构的知识有一个较为全面的了解，并在今后的学习和工作中学以致用，尽快地成长为信息安全某个具体领域的专家，为我国的信息安全事业作出贡献。

本书在写作过程中得到了清华大学出版社的大力支持和国家重点基础研究发展规划项目(项目编号：2007CB311202)的资助，也得到了业界同行的鼓励和帮助，在此表示衷心的感谢。

作者

目 录

第1章 概 述

1.1 基本概念

1.1.1 体系结构

什么是体系结构?它是由英文单词 architecture 翻译而来。在英语中,architecture 最常用的解释就是“建筑”。可见,与任何一个“建筑”相类似,一个体系结构应该包括一组组件以及组件之间的联系。从系统工程的观点来看,任何复杂的系统都是由相对简单的、具有层次结构的基本元素组成。这些基本元素彼此之间存在着复杂的相互作用,某些元素还可能具有非常复杂的内部结构。

上述的朴素解释能够帮助我们理解体系结构的重点所在,即元素及其关系。在更为严格的学术意义上的解释中,各类体系结构的侧重点不一而同地都落在“元素及其关系”这几个看似简单的字上。例如,ANSI/IEEE STD 1471-2000 使用的体系结构的定义是:“一个系统的基本组织,通过组件、组件之间和组件与环境之间的关系以及管理其设计和演变的原则具体体现。”这里,“组件”即前面所说的“元素”,“组件之间和组件与环境之间的关系”即前面强调的“关系”。

1964 年,G. Amdahl 首次提出了“体系结构”的概念。这一概念的产生促使人们对计算机系统开始有了统一而清晰的认识,并进一步为计算机系统的设计与开发奠定了基础。四十多年过去了,体系结构已经与系统软件、应用软件和程序设计语言有了紧密结合,并且相互作用。伴随着计算机科学、网络与通信技术的飞速发展,围绕体系结构的研究与应用也得以迅速发展,内涵和外延都得到了极大的丰富,涉及网络计算、芯片设计、信息安全产品研发与应用等领域。例如,网络计算体系结构已经成为一种主要的计算模式,芯片级体系结构的研究也是当前一个具有很大挑战性的问题。

目前,对于体系结构的定义,结合前面的最基本定义,不同的机构有着不尽相同的具体定义。例如,信息管理体系结构(TAFIM)提出了一个技术体系结构的定义,即“组件、接口、服务及其相互作用的框架”,从软件工程的角度提出了描述信息系统的四个视图,即“计算视图、数据管理视图、通信视图、安全视图”。开放组织体系结构框架(TOGAF)认

为体系结构包括基础体系结构、标准信息库和体系结构开发方法(ADM),并在此基础上定义了体系结构描述标记语言 ADML。IEEE 的体系结构计划研究组(APG)指出,体系结构可以被认为是“组件+连接关系+约束规则”,并建议针对体系结构的描述建立指导性文档。

一般来说,最常见的关于体系结构的分类是将其分为硬件体系结构和软件体系结构两大类。

硬件体系结构的定义由计算机科学中的计算机体系结构发展而来。在计算机科学中,硬件体系结构通常包含了计算机组成原理与设计、计算机系统结构、数字逻辑与数字电路等一系列内容。其中,计算机组成原理与设计是指根据各种计算模型研究计算机的工作原理,并按照器件、设备和工艺条件来设计、制造具体的计算机;计算机系统结构是指对计算机系统的软件、硬件功能进行分配;数字逻辑与数字电路主要涉及数制、码制和逻辑代数,以逻辑代数为工具,对各类组合电路、同步时序电路、异步时序电路的基本逻辑单元进行分析和设计,并对存储器和可编程逻辑器件的性能和特点进行刻画。由于这里提到的各种“元素”,大多是客观可见的组件,例如,逻辑电路元器件。总的来说,硬件体系结构比较容易理解。

随着各种计算机硬件产品(例如,硬件防火墙、硬件 VPN 等)的出现,硬件体系结构不再局限于计算机科学领域,而是成为这些多样化的硬件产品设计、实现、应用和维护过程中不断出现的术语,指的是这些硬件的物理组成部件及其相互关系。当然,这里的“物理组成部件”与计算机体系结构中的“元素”有很多相同之处。

通俗地讲,软件体系结构指的是软件系统在其分析和设计过程中确立的系统中基本元素相互作用的方式。这些基本元素是实现软件系统功能必须的元素。严格地讲,软件体系结构是具有一定形式的结构化元素,即构件的集合,包括处理构件、数据构件和连接构件。处理构件负责对数据进行加工,数据构件是被加工的信息,连接构件把体系结构的不同部分组合连接起来。这一定义注重区分处理构件、数据构件和连接构件,这一方法在其他的定义和方法中基本上得到了保持。

与上述分类方法不同的是,信息系统体系结构则不再区分为硬件和软件,而是从信息系统设计与开发的角度,考虑其组成元素及其彼此间的关联和相互作用。

另外一个经常出现的相关概念是企业体系结构(EA)。这是帮助一个企业理解自己的组成结构及其原理的概念性工具。企业体系结构提供了企业的结构图,是企业业务和技术变化的规划工具。一般来说,企业体系结构表现为一整套相互关联的模型,这些模型描述了企业的结构和功能。企业体系结构主要用于系统化的信息技术规划和架构,以及对它们进行改进的决策过程。EA 中的各个模型以逻辑方式排列,可以使企业的详细信息处于不断增长的过程中。这些信息包括目的和目标、过程和组织、系统和数据以及使用的技术。

体系结构有以下六种基本的模式。

1）管道和过滤器

在这种模式下，每个组件具有输入和输出的数据流集合，从该集合的某个数据流中读数据作为输入，产生输出数据流，整个系统可以被看成多个过滤器复合形成的数据处理组件。一个最著名的实例是 UNIX 的 shell 编程，多个对数据进行处理的程序（组件）通过管道联结起来，产生总和的效果。另一个例子是传统的编译器，源代码经过词法分析、语法分析、中间代码生成、目标代码生成等步骤生成输出的目标代码。

2）数据抽象和面向对象

在这种模式下，数据和数据上的操作被封装成抽象数据类型或者对象。系统由大量的对象组成，在物理上，对象之间通过函数或者过程调用相互作用；在逻辑上，对象之间通过集成、复合等方式实现设计的复用。

3）事件驱动

它是上述第二种模式的一种变形。在这种模式下，系统同样是由大量的对象组成的，但是对象之间的交互不是通过明确指明对象的函数或者过程调用进行的；相反，系统提供事件的创建和发布的机制，对象产生事件，一个或者多个对象通过向系统注册关注这个事件并由此触发出相应的行为或者产生新的事件。一个最著名的例子是 GUI 的模型，鼠标、键盘或者其他输入设备产生各种事件，窗口、程序或者其他对象由这些事件所触发，产生新的事件、进行数据处理或者其他操作。

4）分层次

这种模式将系统功能和组件分成不同的功能层次，一般而言，只有最上层的组件和功能可以被系统外的使用者访问，只有相邻的层次之间才能够有函数调用。ISO 的开放系统互连（OSI）参考模型是最著名的层次模型的例子，通过将开放系统的功能和组件划分成 7 个层次，定义清晰的（很多时候是过于复杂的）层次之间的接口，实现复杂的互操作性。

5）知识库

这种模式使用一个中心数据结构表示系统的当前状态，一组相互独立的组件在中心数据库上进行操作。如果组件负责对中心数据进行选择、处理，这种体系就是传统的数据库模型；如果中心数据结构自主地引发一系列的行为，则这种体系可以被看成一个黑板模型。大量的传统数据库应用程序实际上就是这一体系的具体实例。

6）解释器

这种模式提供面向领域的一组指令（语言），系统解释这种语言，产生相应的行为，用户使用这种指令（语言）完成复杂的操作。大量的开发工具、二次开发工具体现了这一思想。例如，Microsoft 公司在其产品中大量使用的 Visual Basic for Application，以及在

AutoDesk 产品中大量使用的 AutoLisp 语言，实际上就是给用户提供了一种面向领域的语言，然后核心解释执行这一语言的指令和指令序列。从而扩充产品的功能，方便用户按照自己的需要定制系统。

这六种模式各有优点和缺点。最常用的是严格的层次结构、事件驱动的结构、知识库的结构和基于解释器的结构。

在严格的层次结构中，系统可以被清楚地分解成为不同的功能层次，例如，基本的图形库，提供不同层次的绘图接口。这种体系结构适合于系统的功能相对简单，并且可以按照复杂的程度、抽象的程度和硬件平台的关系等方面的特性加以分层的软件中。

事件驱动的结构适用于对互操作性、特别是异构环境下的互操作性要求非常高的情况。当整个系统中存在大量的并发的、相互之间没有逻辑联系的组件的时候可以使用这种体系结构。现代软件技术中微软的 COM 和 ISO 的 CORBA 实际上都采用了这种体系结构。

知识库的结构适用于以大量数据为核心的系统，例如，人工智能的应用系统。如果将面向对象和层次化的思想引入知识库系统中，将得到一种非常强大的体系结构。

基于解释器的结构适用于应用系统和用户的交互非常复杂的情况。只有将系统的基本操作以指令的形式提供给用户，同时，提供一种简单明了的语法和基本的数据操作、处理的功能，才能得到功能最强大、最灵活、具有最佳扩充性的应用系统。例如，浏览器的设计就采用了这种结构。最初，浏览器只是完成下载和显示 HTML 页面的简单工作，随着用户对界面交互要求的提高才开发出 Javascript 这种脚本语言提供功能扩展。

在更多的实际应用中，经常综合采用上面几种体系结构，我们将其称为复合体系结构。例如，可以在系统的某几个部分中采用一种体系结构，而在其他部分采用另外的体系结构。在实际的系统分析和设计过程中，可能首先将整个系统作为一个功能整体进行分析和加以权衡，得出最上层的、合理的体系结构。如果其中的某些元素比较复杂，可以对这些元素继续进行分解，得到一个局部的体系结构。在分析和设计阶段，关注的重点应该是系统的总体结构，避免过多地关注具体的实现细节（例如，所应引入和使用的语言、具体需要的技术等）。

借鉴软件工程中的相关知识，对体系结构的描述经常采用视图的方法，并且主要有三类视图，即物理视图、逻辑视图和概念视图。体系结构中的每一层都可能有多个视图，而且事实的确如此。体系结构设计师需要结合与体系结构设计相关的功能要求、操作要求，选择采用合理的模式进行设计和开发工作。例如，对于应用程序结构设计师而言，每个应用程序通常都会有一个逻辑应用程序结构。这些视图由一组需求来驱动，反过来又会生成设计、开发、配置和运作过程及系统的输入，如图 1-1-1 所示。

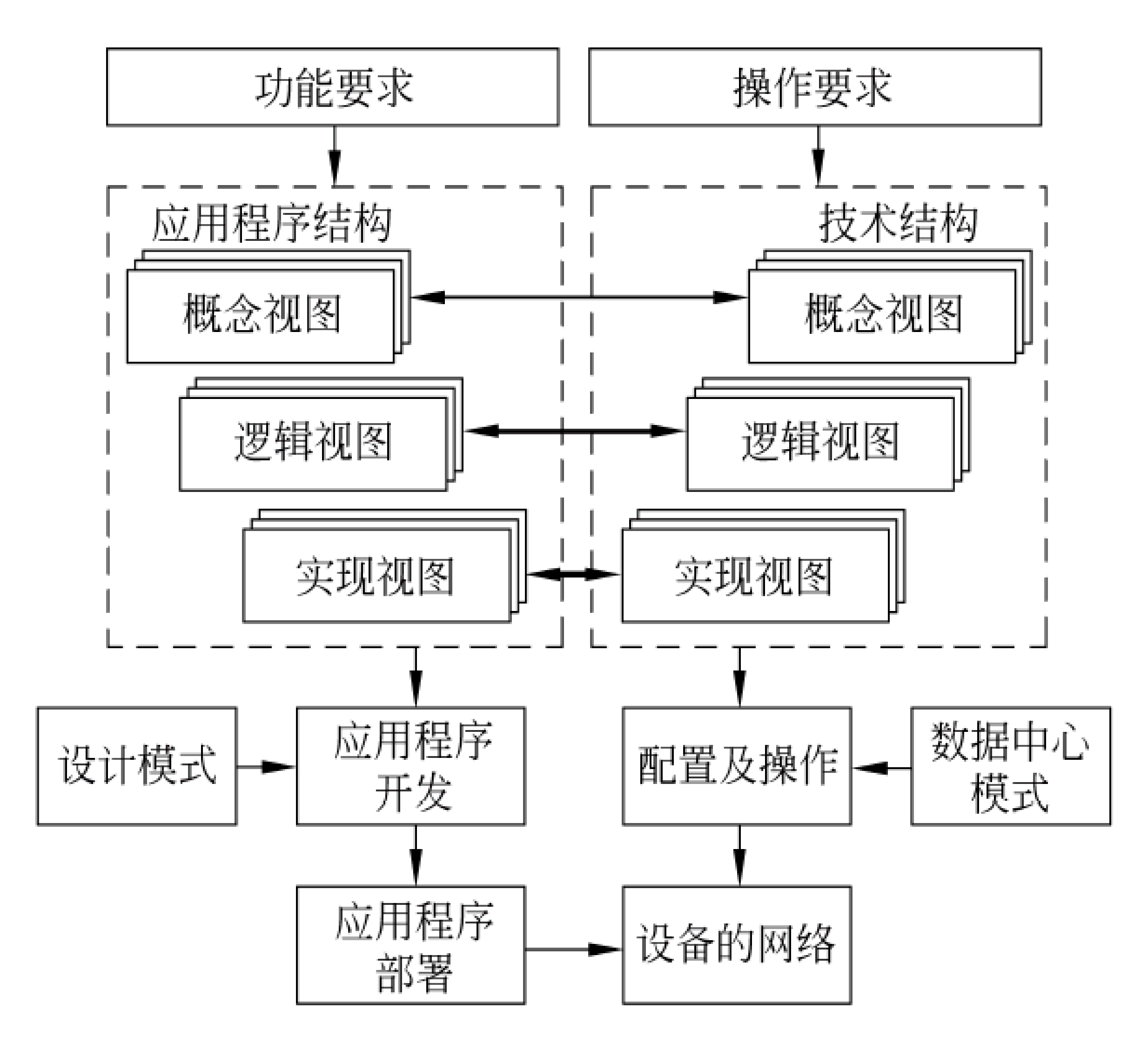


图 1-1-1 应用程序体系结构中的视图

1.1.2 信息安全体系结构

这里所说的信息安全体系结构是针对信息系统而言的。一般地，信息系统的安全体系结构是系统信息安全功能定义、设计、实施和验证的基础。该体系结构应该在反映整个信息系统安全策略的基础上，描述该系统安全组件及其相关组件相互间的逻辑关系与功能分配。这种描述的合理性和准确性将直接关系信息系统安全策略的实现效果。

结合上述基本定义，研究机构 X/Opengroup 认为，信息系统的安全体系结构是系统整体体系结构描述的一部分，应该包括一组相互依赖、协作的安全功能相关元素的最高层描述与配置，这些元素共同实施系统的安全策略。

美国国防部则开展了更为全面的研究工作。1996 年，它结合以往的工作经验和实际需求，在一项研究中将信息安全体系结构分成了四类，各类结构的定义和特点如下。

1）抽象的安全体系结构

描述安全需求，定义安全策略，选择相应的安全服务/功能，在抽象定义的信息系统体系结构的组件之间分配安全功能。

2）通用的安全体系结构

基于抽象的安全体系结构，定义通用类型的安全组件和允许使用的标准，并为其应用确立必要的指导原则；在安全服务/功能分配的基础上，定义实现一定安全强度的安全服务类型和安全机制。

3）逻辑的安全体系结构

为某种真实、具体的安全需求而设计，是在具体环境中应用通用的安全体系结构的实例，同时必须分析实施代价。

4）具体的安全体系结构

关注组件、接口、标准、性能、代价，展示所有选择的组件、机制、规则等如何结合并满足特定系统的安全需求。

围绕上述定义和分类，许多研究机构、技术组织，以及美国国防部之类的国家性机构，相继进行了进一步的研究活动，并在其相应的标准化或技术实践中表达了各自的观点。

其中，国际标准化组织和国际电工委员会提出了所谓的“OSI 安全体系结构”，结合其著名的开放系统互连模型（OSI 参考模型），认为安全体系结构应该是安全服务与安全机制的一般性描述，说明怎样将安全服务映射到网络层次结构中，简单讨论了这些安全服务在其中的适当层次，应该包括可信功能度、安全标签、事件检测、安全审计跟踪、安全恢复等与安全管理相关的普适性机制。

X/Opengroup 提出了一种“分布式系统安全框架（XDSF）”，将安全功能元素分成了三个层次，即最底层的密码支持硬件或软件，中间层的基本安全功能（包括认证、授权、审计等），最上层的（域间交互的）安全服务（包括特权属性服务、证书服务、密钥分发、可信第三方等）。在这样一个框架中，安全管理覆盖了对于上述三个层次中所有安全元素的管理。

美国国防部提出的“目标安全体系结构（DGSA）”在 OSI 安全框架的基础上，从物理组成的角度，分析信息系统各组件彼此间的安全功能分配问题。在该结构中，主要的物理组成实体是端系统、中继系统、传输网络、本地通信系统、本地用户环境，安全需求则是在美国国防部以前提出的信息系统安全需求基础上形成的一定层次上的抽象，具体包括支持多种信息安全策略、采用开放系统、实施充分的保护，以及实现共同的安全管理。美国的信息系统防卫局（Defense Information Systems Agency，DISA）提出的美国国防部信息系统安全计划（DISSP）认为信息安全体系结构应该是一个三维的矩阵结构框架，每一维分别代表了安全属性、OSI 协议层和系统组件。但是这样一个矩阵状的结构框架具有明显的局限性。首先，系统组件维（包括端系统、接口、网络系统、安全管理）无法反映网络工程中的实际需求；其次，安全属性维也无法表明各属性之间的逻辑关系。

美国国家安全局在信息安全体系结构的研究和开发中进行了许多尝试。它与合作伙伴提出的“DTOS 安全体系结构”作为一个通用系统框架，采用了基于安全威胁的开发方法，建立在 Mach 微内核上，由一个管理器和安全服务器构成。这样一个体系结构在设计上具有一个特点，即以分离方式实施安全判定和判定结果，安全判定由安全服务器进行，而安全判定结果的实施由管理器负责。所以，它能够支持灵活的安全策略。与之类似的是，在与犹他大学合作提出的 Flask 安全体系结构中，对于确定的客体管理器和安全服务

器这两类子系统，该体系结构描述了其相互作用和各自组件的安全要求。其中，安全服务器进行安全策略判定，客体管理器负责实施判定结果。Flask 安全体系结构可以支持安全策略的独立性和动态性。在一些业界支持者（主要是 NAI、SCC、MITRE）的协助和共同努力下，美国国家安全局已经在 Linux 内核中实现了 Flask。

另一个值得一提的信息安全体系结构是通用数据安全体系结构（Common Data Security Architecture，CDSA）。它由 Intel 体系结构实验室（Intel Architecture Labs，IAL）提出，并得到了 Apple、Entrust、Hewlett-Packard、IBM、Motorola、Netscape、Sun、Trusted Information Systems 以及 PKI Task Group 许多成员组织的参与和大力支持。它定义了一组分层的安全服务和应用程序接口，为 Internet 的数据与通信安全应用提供动态的、集成化的安全服务。CDSA 是一个开放的、可扩展的体系。由于各应用程序可自由选择、动态访问该体系中的服务，CDSA 可以为不同的用户提供多平台、多层次、多密级的信息安全服务。

CDSA 有三个基本的层次：系统安全服务层、通用安全服务管理器（CSSM）层、安全模块层（密码服务、信任策略、证书库、数据存储库、授权计算等模块）。其中，CSSM 是 CDSA 的核心，负责对各种安全服务进行管理，管理这些服务的实现模块。CSSM 定义了访问安全服务的应用编程接口，为安全服务模块规定了服务提供接口（SPI），动态地为应用扩展所需的安全服务，控制着可信计算机的核心，监视着动态环境的完整性。其体系结构如图 1-1-2 所示。

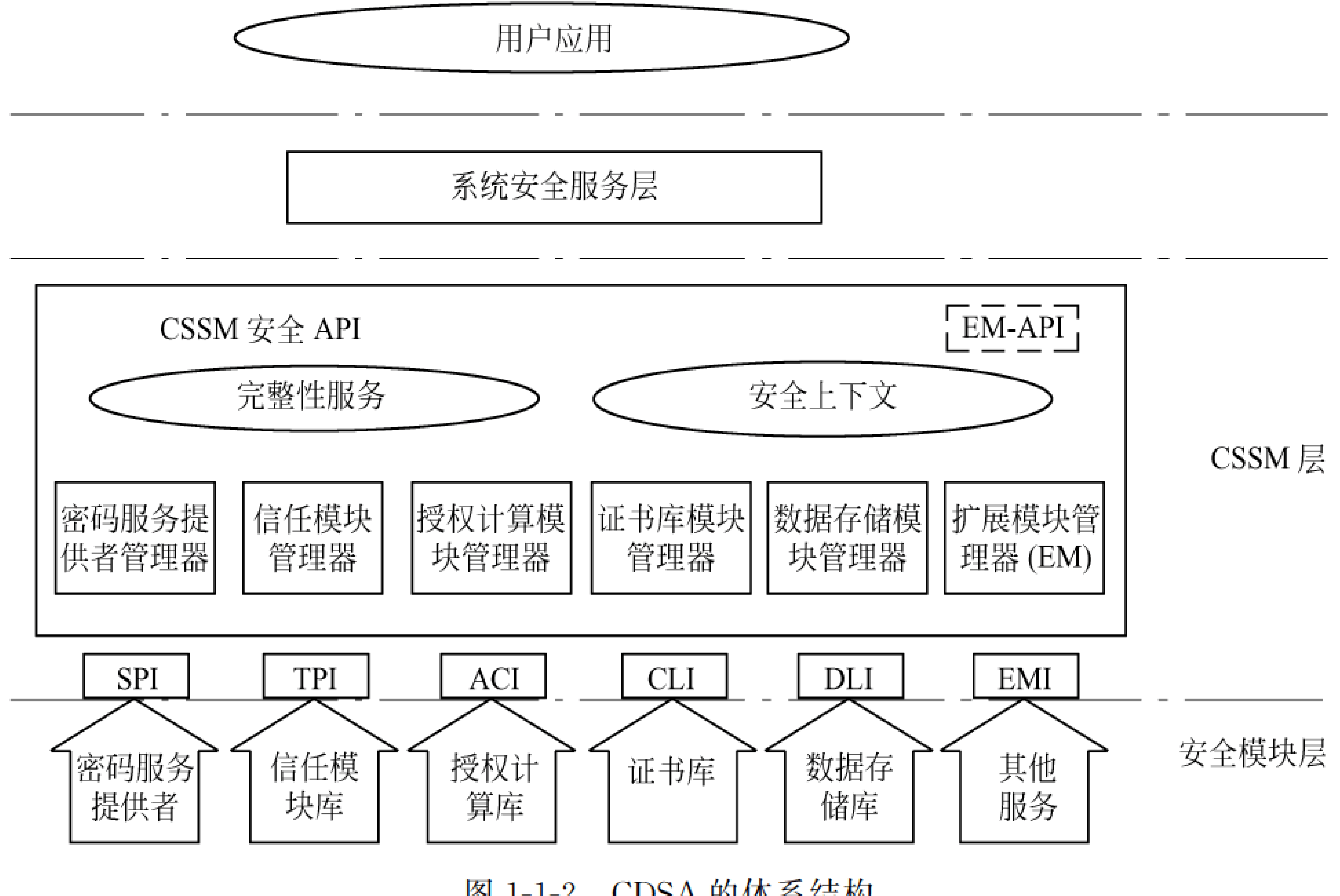


图 1-1-2　CDSA 的体系结构

本书对于信息安全体系结构的定义，采用了美国 Greenwich Technology Partners 公司信息安全小组的实践领导人 Christopher M. King 在其与他人合著的《安全体系结构的设计、部署与操作》中对于信息安全体系结构给出的定义，即：信息安全体系结构是由安全技术及其配置所构成的安全性集中解决方案。

这样的一个定义表明，信息安全体系结构在设计、实施、应用的过程中，需要考虑许多相关的问题，与具体应用需求的整个生命周期有关。例如，必须进行需求分析，制定和实施相关的安全策略；必须仔细考虑如何合理应用网络隔离、平台加固、VPN、IDS、PKI、恶意代码防范等众多信息安全技术与相关产品；必须全面衡量解决方案的具体实施过程所涉及的系统操作、运行与管理等方面的有关问题。

1.1.3　信息安全保障

随着信息安全的概念由早期的信息保密逐步发展到今天的信息安全保障(Information Assurance，IA)，人们对于信息安全保障的概念需要在此前众说纷纭的基础上加以统一。

在国外，“信息安全保障”这一概念最早出现在 1996 年美国国防部的国防部令 S-3600.1 中。国防部令 S-3600.1 将“信息安全保障”明确定义为“保护和防御信息及信息系统，确保其可用性、完整性、机密性、可认证性、不可否认性等特性。这包括在信息系统中融入保护、检测、响应功能，并提供信息系统的恢复功能。”这个定义明确了可用性、完整性、可认证性、机密性和不可否认性这五个基本的信息安全属性，提出了保护(Protect)、检测(Detect)、响应(React)、恢复(Restore)这四个动态的信息安全环节(如图 1-1-3 所示)，强调了信息安全保障的范畴不仅仅是对信息的保障，也包括对信息系统的保障。在美国，这个“信息安全保障”定义沿用至今。事实已经表明，与早期信息安全的概念相比较而言，它更符合现在客观的信息安全需求。

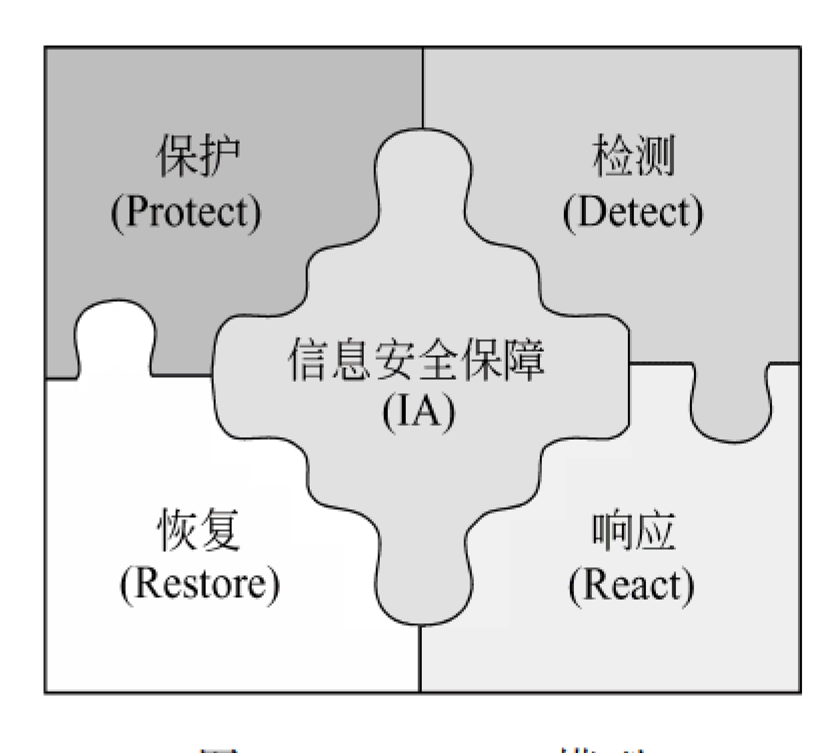


图 1-1-3　PDRR 模型

在我国，从有关专家学者开始关注美国国家安全局 2001 年发布的《信息安全保障技术框架(2.0 版)》(Information Assurance Technology Framework)开始，对信息安全保障概念已经经历了多年的探讨。直到今天，无论是在学术界、管理部门，还是产业界，对这个概念的理解仍然没有统一。早在信息安全国家重点实验室的专家组织国内多所高校的相关专业的教学科研人员翻译《信息安全保障技术框架》时，就不断地有地方和军队的专家指出，他们对“保障”一词的翻译有不同的见解。这些见解主要有三种：一是主张改用“防

御”或者“防范”，以便强调追求信息安全的自信；二是认为“保障”的说法容易使人将其与军事术语“后勤保障”相联系，并在此基础上减弱“信息安全保障”的重要性；三是指出“信息安全保障”这一词语的出现，容易使人联系到情报工作中的情报保障概念。另外一些人则喜欢使用“信息保障”这一概念，是其英文的直接翻译。实际上，无论翻译文字如何，想表明的是，当前信息安全的内涵需要体现未雨绸缪、积极防御的思想。

目前，我国大多数研究人员还比较认可下述关于“信息安全保障”的定义：信息安全保障是对信息和信息系统的安全属性及功能、效率进行保障的动态行为过程。它运用源于人、管理、技术等因素所形成的预警能力、保护能力、检测能力、响应能力、恢复能力和反击能力，在信息和系统生命周期全过程的各个状态下，保证信息内容、计算环境、边界与连接、网络基础设施的真实性、可用性、完整性、机密性、可控性、不可否认性等安全属性，从而保障应用服务的效率和效益，促进信息化的可持续健康发展。

这个定义明确了两个工作对象（信息和信息系统）、五个安全属性（可用性、完整性、可认证性、机密性和不可否认性）、四个工作环节（保护、检测、响应、恢复）、四个信息保障的对象（信息内容、计算环境、边界与连接、网络基础设施），以及信息保障的核心（应用服务）。但是没有涉及信息和信息系统的状态和信息保障能力的来源问题。

如果抛开上述过多的术语来解释什么是信息安全保障，有一个非常容易理解的说法，那就是：所谓信息安全保障，就是人利用技术和管理来实现信息安全的这样一个过程。这里，可以看到，信息安全保障具有三个要素：人、技术和管理。

1.2 三要素

1.2.1 人

时至今日，随着人们对信息安全重视程度的提高，“人是第一位的”已经成为一个逐渐被接受的观点。前面我们提到了信息安全保障。人是信息安全保障关注的三要素之一。这里所说的人，包括信息安全保障目标的实现过程中所有的相关人员，例如，机构信息安全保障目标的制定与实施人员，业务系统的设计、开发、维护与管理人员，这些系统（或产品）的用户，可能存在的网络入侵人员，信息安全事件报告、分析、处理人员，信息安全法律顾问等。

在信息安全发展的早期阶段，我们关注的重点是技术和产品，对于新技术、新产品的出现和他们所能发挥的作用给予了过高的期望。结果是，技术的种类与名目越来越多，产品的功能和形式也五花八门，各种各样的信息安全事件或事故却也与日俱增。静下心来

仔细想想，如果没有某些人(例如，粗心的用户，有意或无意造成破坏的设计者，安全意识淡漠的管理人员等)的介入，或许这些技术和产品的实际功用真的会更大，更让我们有乐观的理由。但是，这可能吗？这些人的影响无处不在。可我们对于这种影响司空见惯了，没有注意到，正是这样一些形形色色的、水平参差不齐的人的介入，使得原本可以更加有用的技术和产品在实际的效用上大打折扣。当然，也因为设计与开发人员的水平有限，某些技术和产品面世的同时就在技术或功能方面具备了某些局限性。

在 IATF 提出的"纵深防御战略"中，与"人"相关的需要考虑的因素有：策略和流程、培训和意识培养、系统安全管理、物理安全、人员安全和设施对策等，如图 1-2-1 所示。在这六个因素的基础上，争取实现的目标是雇用优秀的人员，给予其良好的培训和报酬，同时也惩罚非授权的行为。

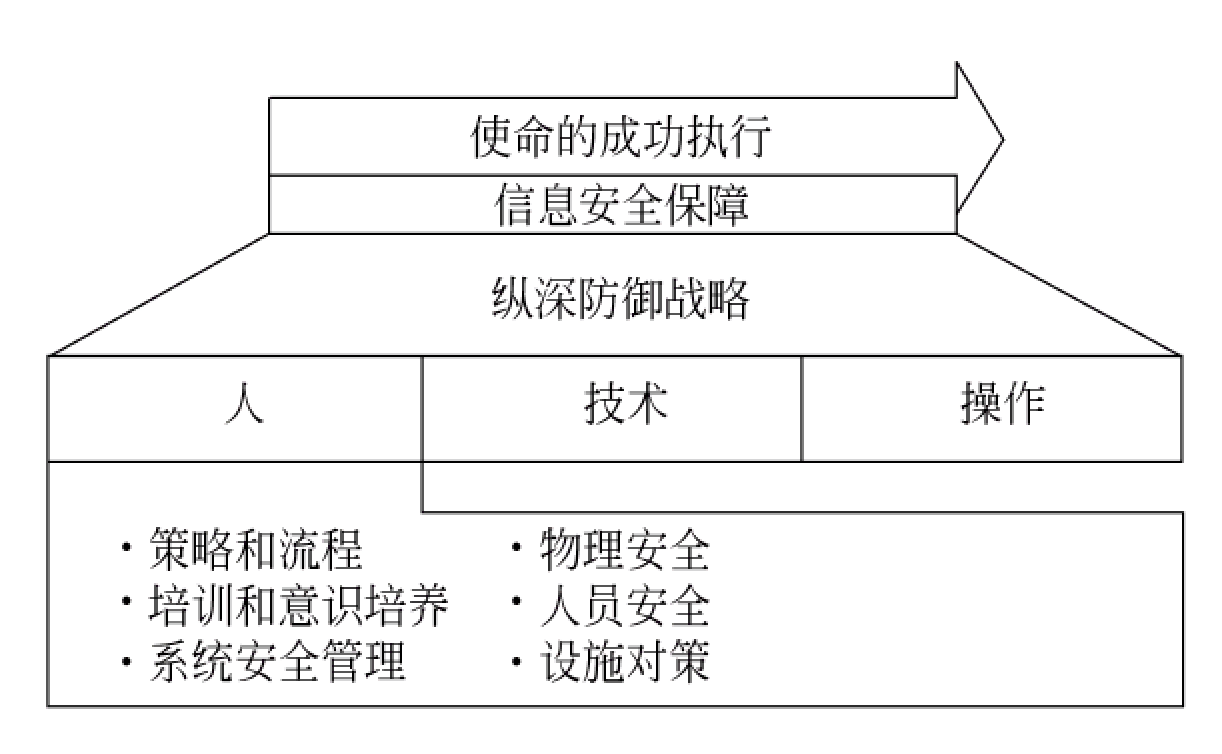


图 1-2-1　纵深防御战略的要素之一：人

现实的情况是，对于任何一个企业或者机构而言，在人这个环节，除了可以预见的不合格内部员工、恶意的竞争者、不合格的合作方，以及对信息安全缺少足够重视的管理者，可能对该企业(机构)造成信息安全的危害之外，一个主要的威胁就来自不可预见的网络世界。这里，有太多的好奇者、好事者，以各种各样的方式，在尝试进入别人的系统，有的仅仅是好奇或者逞能地看一看，有的则是有意图获得对自己有用的数据或者进行纯粹的破坏。

那么，怎样才能如愿以偿，获得具备应有素质的人呢？

NIST 在 1998 年 4 月颁布了特别出版物 SP 800-16《信息技术安全培训要求：任务和实现的基本模型》。这个出版物对意识、培训、教育的一些特点进行了比较(见表 1-2-1)。

表 1-2-1　对意识、培训、教育这三者的比较

比较项目	意　　识	培　　训	教　　育
特征	什么(What)	怎么(How)	为什么(Why)
程度	信息	知识	洞察力

续表

比较项目	意　识	培　训	教　育
学习的目标	认识和记忆	技能	理解
教学方法举例	媒体：视频、时事新闻、张贴宣传品	实践指导：演讲和演示、个案研究、传授实践	理论指导：研讨会和讨论、阅读和学习、研究
测试措施	对/错判断、多选（识别学习）	解决问题、记忆和解答（应用学习）	尝试（理解学习）
影响的时间	短期	中期	长期

早在 1991 年，美国计算机道德规范学会就在华盛顿召开了第一次美国国家计算机道德规范会议。当时，这个学会的主席和奠基人 Ramon C. Barquin 提出了《计算机道德规范的十条戒律》草案，内容是：

(1) 不要使用计算机去做伤害他人的事。

(2) 不要干扰其他人用计算机进行的工作。

(3) 不要窥视他人的计算机文件。

(4) 不要使用计算机进行偷窃。

(5) 不要使用计算机来承担伪证。

(6) 不要复制或使用你没有付款的专有软件。

(7) 不要使用没有授权的计算机资源。

(8) 不要充当他人的枪手。

(9) 要考虑你正在写的程序或你正在设计的系统的社会后果。

(10) 要永远考虑采用一种能够获得你的同伴尊敬的方法使用计算机。

从那之后，这十条戒律就成为计算机道德规范的指南性文件。

即使那些在网上四处张望、热心于迎接技术挑战和解决技术问题的黑客中，也有一些在其内部得以公认的行为守则。违背了这些守则内容的黑客，会遭到同伴的冷眼。例如，一个比较流行的黑客行为守则的内容大致如下：

- 不恶意破坏任何系统，否则只会给你带来麻烦。恶意破坏他人的软件将遭受法律惩罚。如果你只是使用对方的计算机，那就仅仅是非法使用。注意，千万不要破坏别人的软件或资料。
- 不修改任何系统文档，如果为了进入系统而必须修改它，请将它改回原状。
- 不要轻易将你要黑掉的网站告诉你不信任的朋友。
- 不要在 BBS 上谈论你的这些。
- 在发表文章时不要使用自己的真名。

- 正在实施入侵行为时不要随意离开自己的计算机。
- 不要侵入或破坏政府机关的主机。
- 不要在电话中谈论这些事情。
- 把笔记放在安全的地方。
- 想要成为黑客就要真正实践，读遍所有有关系统安全或系统漏洞的文件。
- 不要清除或修改已被侵入的计算机中的账号。
- 不要修改系统档案（为了隐藏自己的侵入而进行的修改例外），但仍需保证系统原有的安全性，不要在得到系统的控制权之后将其门户大开。
- 不要和朋友分享你已经破解的账号。

第 7 章将介绍有助于企业和机构衡量和提升人员水平的人员能力成熟度模型。

1.22　技术

在传统的观念中，技术始终是信息安全中最重要的话题。早期，在信息化普及程度不高的背景下，采用了先进的信息安全技术的信息系统，面临的风险确实要小一些。但是，这些年情况已经发生了变化。

原因很简单，那就是任何一个新技术的引进，任何一个新产品的加入，如果有对其精通的人故意作对，或者无意而为，都会带来新的隐患。

追求技术的发展和产品的更新无可厚非。但如果要更安全，就要对这些技术和产品具有相当的了解和控制权，使它们能够为自己服务，而不是被他人利用。

纵深防御战略对技术的相关元素进行了描述，如图 1-2-2 所示，其核心是采用经过评估的产品和解决方案，支持分层的防御战略。

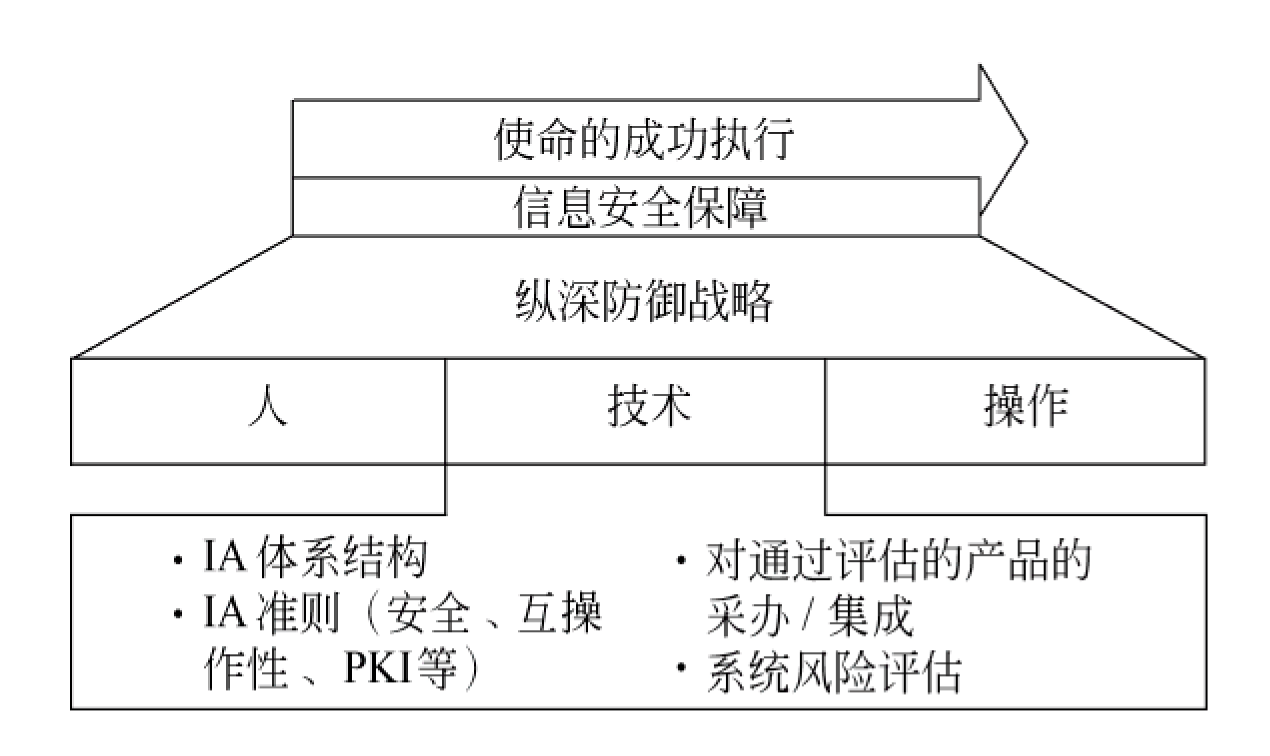


图 1-2-2　纵深防御战略的要素之一：技术

IATF 中认为，现阶段，已经有很多可以用于提供信息安全服务和实现信息安全保障目标的技术。为了能够正确运用这些技术和合理部署相关的产品，一个企业或者机构就

必须建立一整套行之有效的技术与产品采购策略和过程，具体包括安全策略、信息保障原则、系统级信息保障体系结构及其标准、信息保障产品选用准则、经可信第三方认证的产品采购原则、产品配置指南，以及系统风险评估过程。

本书的第 3 章将对目前主要的信息安全技术进行介绍，第 4 章将对目前主要的信息安全产品进行介绍。

1.2.3　管理

俗话说，“三分技术，七分管理”。可见管理在信息安全保障中的重要性。“管理”通常指的是对实现信息安全保障目标负有责任的有关人员具有的管理职能，如图 1-2-3 所示。如果从系统运行与维护的角度来看，也可以称之为“操作”或者“运行”。

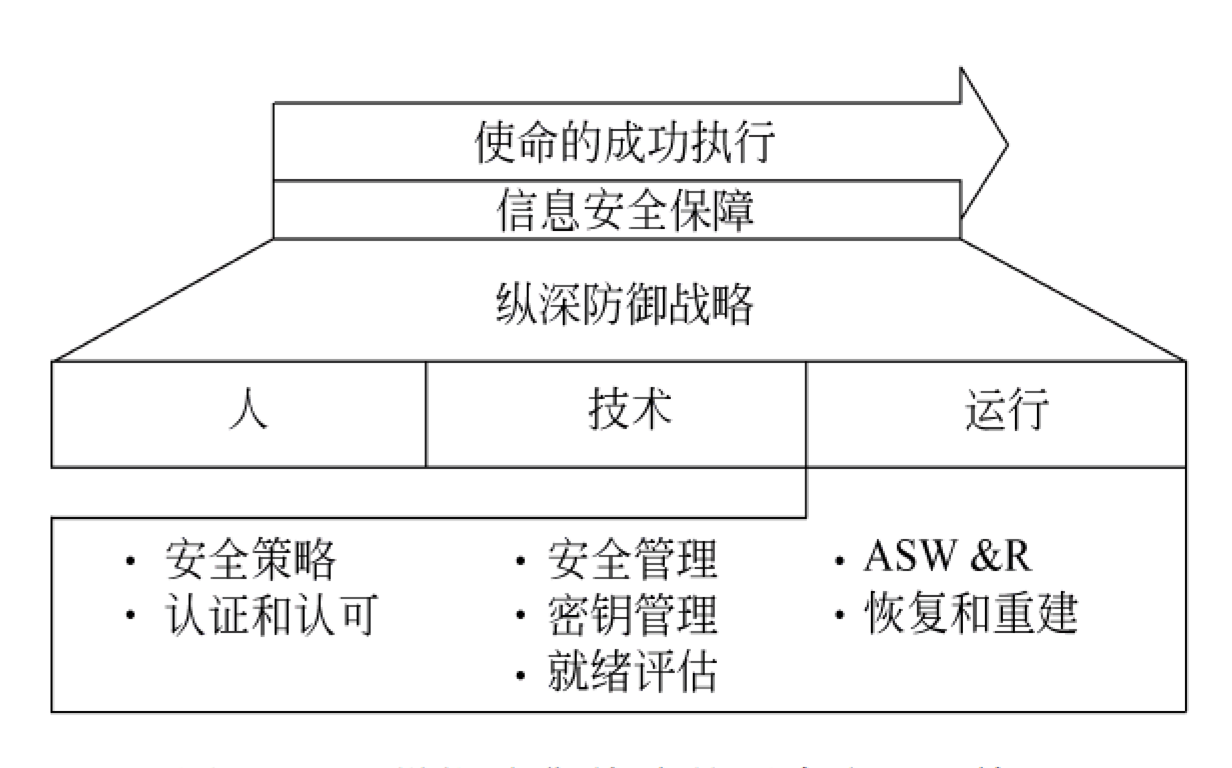


图 1-2-3　纵深防御战略的要素之一：管理

在管理环节中，最重要的是制定和实施符合实际需求的安全策略，即实施安全策略，迅速实施入侵响应，恢复关键服务。2.4 节将介绍有关安全策略的内容。

第 5 章和第 6 章将分别介绍信息安全标准和信息安全管理的相关内容。

1.2.4　三者的相互关系

事实上，上述纵深防御战略已经从一个角度描述了人、技术和管理这三要素之间的关系，那就是：在实现信息安全保障目标的过程中，三个要素相辅相成，缺一不可。

例如，在一家客户众多的商业银行中，为了保证其信息安全状况能够符合业务发展的需要，必须配备相应的专业人员，引进成本恰当、科学合理的新技术和采购功能与性能符合需要的新产品，同时也要制定和实施有效地管理方法与监督流程。人、技术和管理，任何一个环节出了问题，都会给银行带来损失。在人这个环节，可能会存在恶意的内部人员非法侵入未授权的系统，盗取客户资料，或者有这么一个不太负责任的系统操作人员，没有对业务系统的数据进行有效备份；在技术这个环节，可能有那么一台防火墙没有配置得

当,总是拒绝来自远程用户的合理请求,也可能存在若干台系统主机,存在可能被黑客利用的操作系统漏洞;在管理这个环节,可能没有对所有必须接受信息安全培训的人进行有效地培训和考核,也可能缺少对于安全策略的仔细研究和实际演练。总之,似乎只要稍不留神,某个环节就会出问题。事实也的确如此。

那么,怎么样才能确保这三要素彼此配合、共同实现信息安全保障呢?不同现实情况的企业或组织会有不同的做法。但一个显而易见的共同点是:绝对不能存有侥幸的心理,或者出于某种浅显的理由,顾此失彼。

1.3 小结

本章重点介绍了两个内容:一个是信息安全体系结构的基本含义,另一个是信息安全保障中涉及的人、技术和管理这三个要素的基本含义及其相互关系。为了让读者理解信息安全体系结构的基本含义,本章一方面介绍了体系结构的各种定义和六种基本模式,另一方面介绍了各个组织对信息安全体系结构的定义,明确了本书所采用的信息安全体系结构的定义,即信息安全体系结构是由安全技术及其配置所构成的安全性集中解决方案。为了让读者理解人、技术和管理三个要素的基本含义及其相互关系,本章首先介绍了人们对信息安全保障的各种理解,其次介绍了美国国家安全局发布的《信息安全保障技术框架(3.0 版)》中关于纵深防御战略的三个主要层面:人、技术和操作。

习　　题

1. 比较体系结构的各种定义,并说明这些定义之间的异同点,指出其共性要素。
2. 分析体系结构的六种基本模式各自的优缺点,描述最常用的四种结构的特点。
3. 比较信息安全体系结构的各种定义,并说明这些定义之间的异同点。
4. 叙述 PDRR 模型。
5. 叙述信息安全保障的基本含义,阐述信息安全保障的基本要素。
6. 叙述人、技术和管理三个要素的基本含义及其相互关系。
7. 作为一个信息安全工作者,应该遵循哪些道德规范?

第 2 章 信息安全体系结构规划与设计

2.1 网络与信息系统总体结构初步分析

网络与信息系统的总体情况在不同的行业有不同的特点。例如,在医疗行业(主要是医院)的信息化建设中,其局域网大多是一个信息点较为密集的吉比特局域网络系统,所连接的现有数百个信息点为在整个医院内医疗和办公的各部门提供一个快速、方便的信息交流平台,各个部门可以通过这个平台进行交流、查询资料等。就网络的整体建设情况而言,这样一个局域网的物理跨度通常不大,通过吉比特交换机在主干网络上提供吉比特的独享带宽,通过下级交换机与各部门的工作站和服务器连接,并为之提供 100Mb/s 的独享带宽,所有楼层级交换机均与中心交换机相连,即可提供上述的应用服务。就网络的区域划分而言,这样一个局域网通常会划分出两个主要区域:医疗网络和办公网络。其中,医疗网络又可以按照所属的部门、职能、安全重要程度等分为许多子网,包括药品子网、门诊子网、病房子网、中心服务器子网等。

医疗网络为用户提供的应用主要是:

① 内部办公网;

② 文件数据的统一存储;

③ 针对特定的应用在数据库服务器上进行开发;

④ C/S 结构的 Oracle 数据库服务。

办公网络为用户提供的应用主要是:

① 内部办公网;

② 文件数据的统一存储。

在教育行业,随着现代化教学活动的开展和教学机构相互交流的增多,教育机构对通过 Internet/Intranet 网络进行信息交流的需求越来越迫切。为促进教学、方便管理和进一步发挥学生的创造力,校园网络建设已经成为现代教育机构的必然选择。在我国,目前基本上所有的大学都建有自己的校园网络,部分规模大、条件好的中学也建有自己的校园

网。由于用户规模的限制,这些网络大部分属于中小型系统,以园区局域网为主,在网络结构和性能要求方面具有自己的行业特色。

以某中学的校园网络为例,承接此项工程的某高级认证代理商将该校园网分为三级结构:以位于图书馆楼内的校园网控制中心为核心;与校园内各建筑(校园内需要联网的建筑物共 10 座,3 座教学楼、2 座办公楼、1 座综合楼、1 座游泳馆、1 座图书馆楼和 2 座宿舍楼)互连形成园区主干;各建筑物内再扩展面向用户的局域网。园区主干连接为 100Mb/s 或 1000Mb/s,建筑物内部的用户局域网提供到桌面的 10Mb/s 或 100Mb/s 网络带宽。该校园网的整体拓扑结构如图 2-1-1 所示。

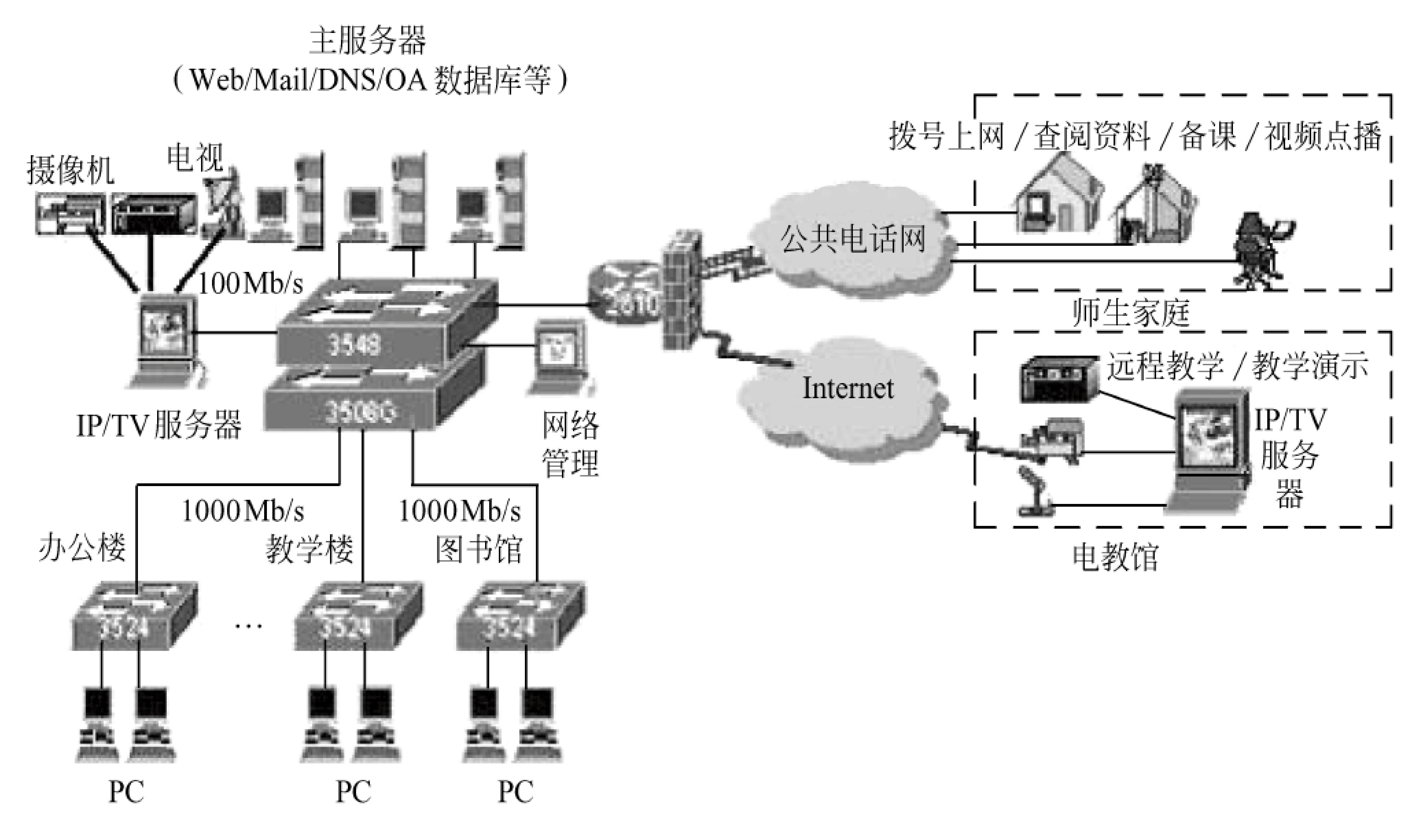


图 2-1-1　某中学校园网拓扑结构图

由两个吉比特级的交换机通过 GigaStack 千兆堆叠,构成校园中心交换机和中心局域网;各建筑物主交换机也选择了千兆级的交换机,控制中心空余的 8 个吉比特端口与 8 栋建筑楼的交换机作千兆光纤连接,剩余的一栋办公楼采用了一条百兆线路与中心连接,至此除网控中心所在的图书馆楼外,其他九栋建筑都与中心连接,形成网络主干;此外,中心 3548 交换机和各楼 3524 交换机的 10Mb/s 或 100Mb/s 局域网端口可以为多台应用服务器提供高速网络连接。这样一种按需求设计带宽和架构的方式,既节省经费,又能充分发挥已购设备的优势,获得最优的整体性价比。建筑物内各楼层采用百兆交换机与本楼主交换机连接,再以 10Mb/s 或 100Mb/s 带宽连接到用户桌面,必要时还可再下联低端交换机扩展用户数。考虑到各交换机都有多个 100Mb/s 端口,级联时可采用 Fast Ether Channel(快速以太网通道)技术,将两交换机的 2～4 对 100Mb/s 或 10/100Mb/s

端口并行连接起来，使级联带宽成倍增加，同时提供线路冗余，其中任一条链路的断线不会妨碍其他链路继续传输数据，从而保障运行的可靠性。此外，为实现 Internet 接入和为在家办公、学习的远程用户提供拨号上网服务，校园网中还在网控中心内设立了 Internet 服务中心，采用路由器(具有 1 个 10Mb/s 以太网接口，2 个 WAN 接口卡和 1 个支持多种模块的网络插槽)作远程连接，其 10Mb/s 以太网端口与网控中心的局域网相连，另可选配一块具备 1 个 2Mb/s 广域网串口的接口卡通过 DDN 专线连接到 Internet；再选配一块 NM-16AM 网络模块，为远程用户提供 16 口拨号连接。

上述两类局域网都属于中小型网络，用户规模在数千人左右，网络建设成本也较高。实际上，在更为简单一些的应用中，网络的建设可以非常简单，例如，某中小型企业的网络拓扑如图 2-1-2 所示。该企业员工数 30 人左右，所建局域网主要是为了方便企业业务的展开和节约成本。企业各部门的计算机通过各自部门的一个集线器接入交换机，负责网络管理的计算机则直接连在交换机上。交换机对外 Internet 的连接上配有防火墙。由于企业内部没有提供对外的公共服务(如电子邮件服务、FTP 服务等)，防火墙也没有设置 DMZ 区。

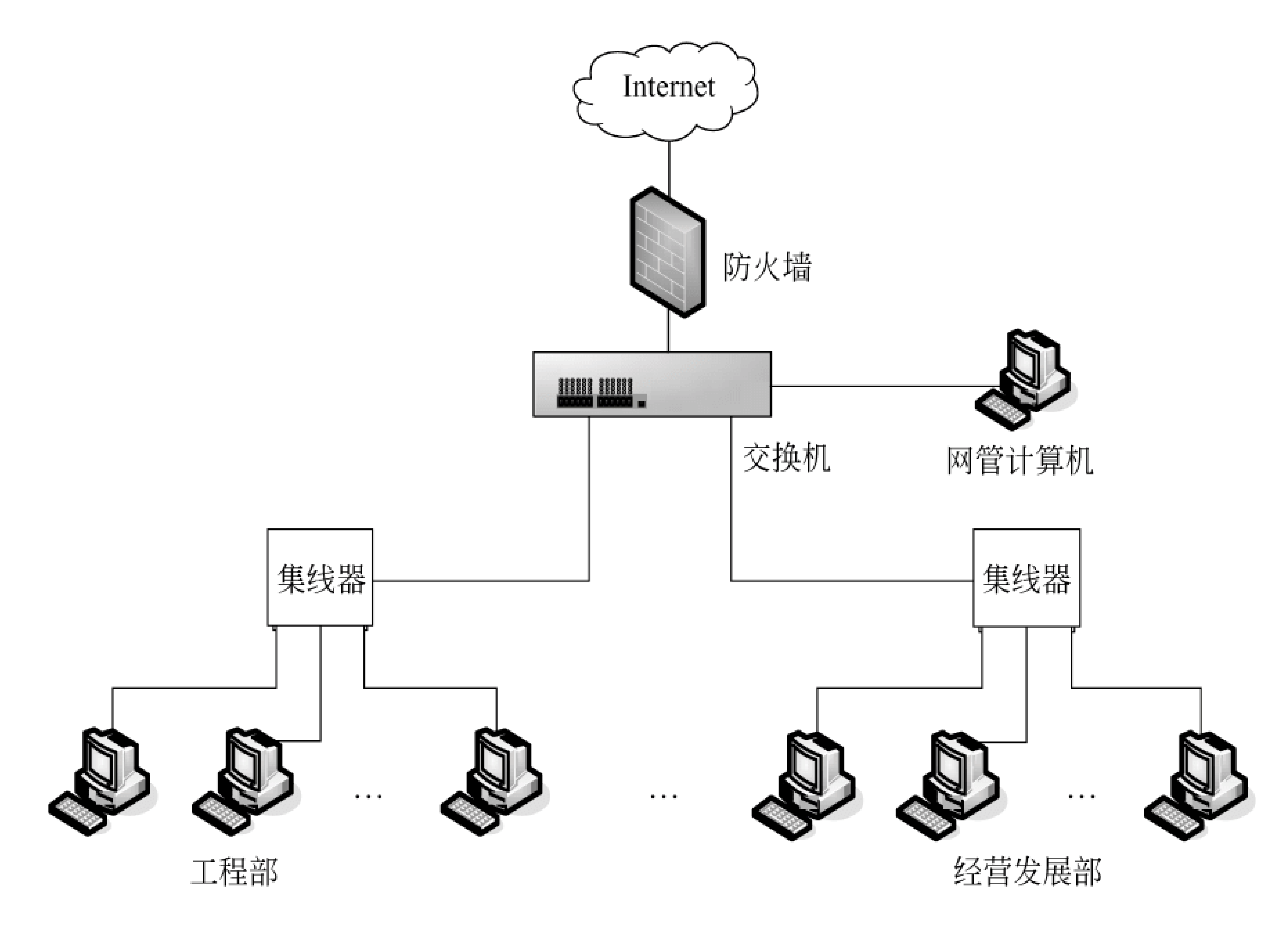


图 2-1-2　某公司局域网拓扑图

对于网络与信息系统的总体情况而言，用户规模、业务量大小，以及建设的成本预算情况，共同决定了网络建设的规模和建设与开发成本。

一般地，越是大型的网络，其结构越为复杂，涉及的人、技术、管理因素越多，可能存在的隐患也就越多。为了确保这些网络的安全，首先就要结合网络使用方的需求和网络建

设者的能力，从设计之初开始准确地判断其信息安全需求，并在设计、实施、应用和维护的全过程中，结合有效地安全策略及其实施方法，合理部署必要的信息安全产品，将可能存在的风险控制在可以接受的范围之内。

这里值得一提的是，将网络安全纳入到信息安全之中，也是学术界和产业界的基本共识。这样，自然而然地也就将网络系统纳入到信息系统之中。信息系统有其自身的含义。一般地，信息系统是由计算机及其相关的和配套的设备、设施（含网络）构成的，按照一定的应用目标和规则对信息进行采集、加工、存储、传输、检索等处理的人机系统，也称计算机信息系统。

2.2　信息安全需求分析

信息安全需求分析贯穿在信息安全体系结构设计与实施的整个过程中，而设计开始之前的需求分析尤其重要。需求分析涉及物理安全、系统安全、网络安全、数据安全、应用安全与安全管理等多个层面，既与安全策略的制定和安全等级的确定有关，又与信息安全技术和产品的特点有关。

221　物理安全

物理安全主要从外界环境、基础设施、运行硬件、介质等方面为信息系统安全运行提供基本的底层支撑和保障。实现物理安全的主要目的是保障存放计算机与网络设备的机房、信息系统设备和数据存储介质等免受物理环境、自然灾害以及人为操作失误和恶意操作等各种威胁所产生的攻击。物理安全是整个信息系统安全的基础。

物理安全需求主要包括：

(1) 物理位置的选择，需要充分考虑周边的整体环境以及所选择的物理位置是否能够为信息系统的运行提供物理上的基本保障。

(2) 物理访问控制，需要对内部授权人员和临时外部人员进出系统物理环境进行控制。

(3) 防盗窃和防破坏，需要考虑机房内部的设备、介质和通信线缆等的安全性，如设立防盗报警、监控报警等装置。

(4) 防雷电，需要考虑防止雷电对电流、设备等造成的不利影响。

(5) 防火，需要考虑防止火灾发生以及火灾发生后能够及时灭火的措施。

(6) 防静电，需要考虑防止静电的措施，以避免产生静电及其对设备和人员等造成的伤害，以及如何减少这种伤害。

(7) 温度与湿度控制,需要考虑保障各种设备正常运行的温度和湿度范围。

(8) 电力供应,需要考虑防止电源出现故障、电力波动范围过大的措施。

(9) 电磁防护,需要考虑防止电磁辐射可能造成的信息被窃取或泄露的措施。

222　系统安全

系统安全又称主机系统安全,主要提供安全的操作系统和安全的数据库管理系统,以实现操作系统和数据库管理系统的安全运行,包括服务器、终端/工作站等在内的计算机设备在操作系统及数据库系统层面的安全。系统安全是保障信息系统安全的中坚力量。系统安全应从身份鉴别、安全标记、访问控制、可信路径、安全审计、剩余信息保护、入侵防范、恶意代码防范和资源控制等方面考虑其安全性需求。下面将在此基础上从以下六个角度介绍系统安全的安全需求。

1. 操作系统、数据库系统、服务器安全需求

操作系统、数据库系统和服务器的安全需求与应用层安全密切相关,这表现在两个方面。一方面,目前广泛使用的这些系统普遍缺少足够的可信任性,或者仅提供很有限的信任或安全机制,难以提供应用层所需的足够的安全机制。另一方面,由于这些系统通常是以软件处理的方式对网络端口做出响应,而软件处理又往往在应用层安全机制的控制能力之外,这些系统更容易遭受网络攻击。

不同安全级别的操作系统、数据库系统、服务器具有不同的安全需求。一般地,设计安全需求的应用系统采用的至少是符合 GB 17859 中的第二级(系统审计保护级)或第三级(安全标记保护级)安全需求的操作系统、数据库系统和服务器。这些安全需求都是通过描述该级别系统的可信计算机的安全要求体现出来的。

1) GB 17859 中的第二级:系统审计保护级

系统审计保护级的安全需求主要包括:

(1) 访问控制。主要保证对系统(操作系统、数据库系统、服务器)资源进行受控合法的使用。这一级采用自主访问控制,即由可信计算机定义和控制系统中命名用户对命名客体的访问。自主访问控制机制根据用户指定方式或默认方式,阻止非授权用户访问客体。访问控制的粒度是单个用户。实施机制(例如访问控制表)允许命名用户以用户或用户组的身份规定并控制客体的共享,阻止非授权用户读取敏感信息,控制访问权限扩散,没有存取权的用户只被允许由授权用户指定对客体的访问权。

(2) 身份鉴别。主要对系统中的每个用户或与之相连的服务器或终端设备进行有效地标识和鉴别。可信计算机初始执行时,首先要求用户标识自己的身份,并使用保护机制(例如口令)来鉴别用户的身份;再有就是要阻止非授权用户访问用户身份鉴别数据;还有

就是将身份标识与该用户所有可审计行为相关联。

(3) 客体重用。在可信计算机的空闲存储客体空间中，对客体初始指定、分配或再分配一个主体之前，撤销该客体所含信息的所有授权。当主体获得对一个已被释放的客体的访问权时，当前主体不能获得原主体活动所产生的任何信息。

(4) 安全审计。主要对主机进行安全审计，以保持对操作系统、数据库系统、服务器的运行情况以及系统用户行为的跟踪，以便事后追踪分析，可信计算机能创建和维护受保护客体的访问审计跟踪记录，并能阻止非授权的用户对它访问或破坏。审计对象包括的事件有：使用身份鉴别机制，将客体引入用户地址空间(例如打开文件、程序初始化)，删除客体，由操作员、系统管理员或(和)系统安全管理员实施的动作以及其他与系统安全有关的事件。对这些事件的具体审计内容包括：事件的日期和时间、用户、事件类型、事件是否成功。对于身份鉴别事件，审计记录包含请求的来源(例如终端标识符)；对于客体引入用户地址空间的事件及客体删除事件，审计记录包含客体名。对不能由计算机信息系统可信计算机独立分辨的审计事件，审计机制提供审计记录接口，可由授权主体调用。这些审计记录区别于计算机信息系统可信计算机独立分辨的审计记录。

(5) 数据完整性。可信计算机通过自主完整性策略，阻止非授权用户修改或破坏敏感信息。

2) GB 17859 中的第三级：安全标记保护级

安全标记保护级的安全需求主要包括：

(1) 访问控制。在系统审计保护级自主访问控制的基础上实施强制访问控制，即由可信计算机对所有主体及其所控制的客体(例如进程、文件、段、设备)实施强制访问控制，为这些主体及客体指定敏感标记。

(2) 安全标记。主要通过对主体和客体进行标记以增强访问控制力度，可信计算机应维护与主体及其控制的存储客体(例如进程、文件、段、设备)相关的敏感标记(这些标记是实施强制访问的基础)；为了输入未加安全标记的数据，可信计算机向授权用户要求并接受这些数据的安全级别，并且可交由可信计算机进行审计。

(3) 身份鉴别。可信计算机初始执行时，首先要求用户标识自己的身份，并且可信计算机维护用户身份识别数据并确定用户访问权及授权数据；可信计算机使用这些数据鉴别用户身份，并使用保护机制(例如口令)来鉴别用户的身份；阻止非授权用户访问用户身份鉴别数据；将身份标识与该用户所有可审计行为相关联。

(4) 客体重用。在可信计算机的空闲存储客体空间中，对客体指定、分配或再分配一个主体之前，撤销客体所含信息的所有授权；当主体获得对一个已被释放的客体的访问权时，当前主体不能获得原主体活动所产生的任何信息。

(5) 安全审计。可信计算机能创建和维护受保护客体的访问审计跟踪记录，并能阻

止非授权的用户对它访问或破坏。审计对象包括的事件有：使用身份鉴别机制，将客体引入用户地址空间（例如打开文件、程序初始化），删除客体，由操作员、系统管理员或（和）系统安全管理员实施的动作，以及其他与系统安全有关的事件。对这些事件的具体审计内容包括：事件的日期和时间、用户、事件类型、事件是否成功。对于身份鉴别事件，审计记录包含请求的来源（例如终端标识符）；对于客体引入用户地址空间的事件及客体删除事件，审计记录包含客体名及客体的安全级别。此外，可信计算机具有审计更改可读输出记号的能力。对无法由可信计算机独立分辨的审计事件，审计机制提供审计记录接口，可由授权主体调用。这些审计记录区别于可信计算机独立分辨的审计记录。

（6）数据完整性。可信计算机通过自主和强制完整性策略，阻止非授权用户修改或破坏敏感信息。

2 基于主机的入侵检测

基于主机的入侵检测系统的目标是以接近实时的方式识别出网络内部的使用者对某个主机的未经授权的使用、误用或滥用的情况，适合监控特定用户或文件的活动。它的检测对象包括主机和服务器的各个方面的信息，例如操作系统日志文件、存取日志文件、用户应用程序文件、用户定义的应用程序策略等。基于主机的入侵检测系统对个人服务器和应用程序容易配置，能够提供可定制的安全性。

基于主机的入侵检测系统通常作为基于网络的入侵检测系统的补充，其安全需求主要包括：

（1）检测注册表的改动。

（2）能够监视主机上的文件的使用情况。

（3）能够检测文件和消息的完整性（基于密码技术，而非简单的校验和技术）。

（4）具备可定制的系统检查能力。

（5）具备审计过程自动复位能力。

（6）能够支持远程管理。

（7）能够将入侵事件捕获到标准化的数据库系统中。

（8）具有可配置的、自动的、基于规则的响应能力。

（9）能够使审计日志所带来的负载与响应能力保持平衡。

（10）能够向一个集中化的系统管理中心进行报警，并采用电子邮件（或传呼、传真等方式）对用户进行报警。

（11）能够与基于网络的入侵检测系统之间进行集成。

3. 基于主机的漏洞扫描

基于主机的漏洞扫描通过主机扫描器进行。主机扫描器是运行于主机自身中的软件

程序，以周期性的或按需启动的模式运行，在主机系统的内部检测主机的安全状况。

基于主机的漏洞扫描的安全需求主要包括：

(1) 应该选用来源可靠的基于主机的漏洞扫描器，以免无法检测出主机中实际存在的漏洞，或引入新的脆弱性。

(2) 必须确定正确的扫描时间和扫描方式，以免造成类似实际攻击事件所造成的影响。

4. 基于主机的恶意代码检测与防范

基于主机的恶意代码检测与防范的安全需求与基于网络的恶意代码检测与防范的安全需求中的部分需求类似，主要包括：

(1) 能够进行数据完整性检测。

(2) 能够以实时方式或按需进行恶意代码扫描。

(3) 对主机运行产生尽可能小的影响。

(4) 能够通过有关的服务器或控制台对受感染主机进行的必要隔离。

(5) 能够提供相应的响应服务，向网络(或系统)管理员和用户(例如被检测出带有恶意代码的电子邮件的发送者与接收者)报警。

(6) 能够通过网络或者其他方式及时进行版本升级。

5. 基于主机的文件完整性检验

基于主机的文件完整性检验通常是依据事件(例如文件访问)或需求，并采用离线方式和周期性方式进行。文件完整性检验的对象包括系统注册文件、文件权限、安全策略、账号信息等。文件完整性检验通常通过文件完整性检验器进行。

文件完整性检验器的安全需求主要包括：

(1) 能够进行自检。

(2) 每个系统有一个需要被监视的文件或数据结构(包括数据结构和环境，例如 LDAP 和 X.509)的集合。

(3) 支持用户方便地添加需要监视的文件或数据结构。

(4) 标识符的设计采用强密码校验和。

(5) 能够自动恢复“干净的”文件或数据结构。

6. 容灾、备份与恢复

容灾、备份与恢复用于确保系统对灾害、攻击和破坏具备一定的抵抗能力，其安全需求主要包括：

(1) 在进行系统设计时必须考虑面临的各种威胁并制定合理可行的容灾策略(包括采用分布式的体系结构和数据存储方式)，为有效避免任何形式的单点故障，应该适当采

用集群配置。

(2) 采用成本合理、实施有效地备份策略,依据需要建立必要的异地容灾备份中心。

(3) 及时更新系统版本,及时修补已经发现的系统漏洞。

(4) 及时更新老化、不稳定的设备和存储介质。

223 网络安全

网络安全为信息系统能够在安全的网络环境中运行提供支持,一方面,确保网络系统安全运行,提供有效地网络服务;另一方面,确保在网上传输数据的机密性、完整性和可用性等。网络安全应从结构安全、访问控制、安全审计、边界完整性检查、入侵检测与防范、恶意代码检测与防范、网络设备防护等方面全面考虑其安全性需求。下面将从网络上的信息传输安全需求、网络边界防护安全需求,以及网络上的检测与响应安全需求介绍网络安全的安全需求。

1. 信息传输安全需求

信息传输安全需求通常与链路加密技术、VPN 应用,以及无线局域网(WLAN)和微波与卫星网等信息传输途径有关。

链路加密的目的是对传输中的数据流进行加密,以防止通信线路上的信息泄漏、搭线窃听、篡改和破坏。链路加密的特点是侧重于在通信链路上对数据流进行加密(不考虑位于信源和信宿的数据流的加密问题),通过在各种链路上采用不同的加密密钥提供数据安全保护,面向结点,对网络高层主体透明,对高层的协议信息(地址、检错、帧头、帧尾等)都进行加密。一旦采用了链路加密,数据便以密文形式传输。

链路加密通常使用对称密码算法提供点对点式的加密通信,实现措施主要是在链路上配置链路加密设备(主要是各种链路密码机)。例如,在高速调制解调器(modem)之后安装 RS422/V.35 接口的高速信道密码机,实现信道加密。一般情况,链路加密产品主要用于电话网、DDN、专线、卫星点对点通信环境。这些设备包括异步链路密码机和同步线路密码机。其中,异步线路密码机主要用于电话网,同步线路密码机则可用于许多专线环境。密码机对所有用户数据进行加密,用户数据通过通信线路送到另一结点后立即被解密。因为加密后的数据不能进行路由交换,中央结点必须通过解密才能得到路由信息。在加密后的数据不需要进行路由交换的情况下(例如 DDN 专线),用户可以自行选择路由加密设备。

早期的链路加密技术只能保证单链路的安全。在 L2TP 和 PP2P 技术出现后,通过链路加密也能够同时确保多链路的安全。链路加密的优点是实现起来比较容易,只需将一对密码设备安装在两个结点间的通信线路上并使用同样的密钥即可,对数据和报头同

时加密，加密运算在密码设备中实现。链路加密的局限性是：全部报文都以明文形式通过所有结点，在结点上，数据容易受到非法访问或破坏；此外，由于每条链路都需要一对加密设备和一个独立的密钥，在需要保护的链路数目较多时，链路加密的成本也较高。

1）VPN

虚拟专用网（VPN）指的是在公共通信设施的基础上实现的任何专用网络。它可以通过利用公共通信设施或租用通信线路（例如，交换和面向连接的帧中继或 ATM，面向包交换和无连接的 Internet 或 SMDS）、拨号服务（例如基于 ISDN 或数字用户线路 DSL）等方式实现。

采用 VPN 的信息传输安全需求主要包括：

（1）必须支持不同的安全连接策略。

（2）必须保证信息的机密性和完整性。

（3）可以有选择地确保数据完整性（例如对于视频和音频数据的获取在一般情况下对数据完整性没有严格要求）。

（4）能够以安全的方式在网络体系结构不同的网络之间传输信息，能够支持位于不同的网络层和不同的安全保障环境下的网络操作。

（5）由于 VPN 关心的是对外部访问进行控制，为防止通过网络层以上的操作将恶意的内部人员或恶意代码引入网络并造成威胁，需要在 VPN 内部建立安全域，增加防火墙，应用基于终端系统的密码机制，并建立针对隐通道的控制机制。

2）无线局域网

无线局域网的实现方式通常是将笔记本计算机等便携式设备通过无线接入的方式连接到有线插入网络处理器。它主要用于网络用户对网络的可移动性、伸缩性、安装速度、简易和灵活性等方面有重要需求的情况下。为实现对数据包的高效传输，无线局域网采用了 IEEE 802.11 标准。同时，与其他协议不同的是，为确保实时流业务所需的带宽和低干扰、低误码，无线局域网还规定了高级别的优先权并采用了带有优先权的重发机制。除此之外，无线局域网使用的传输协议和数据协议通常与有线网络相同，但是相比而言所需的带宽略低。

无线局域网上同样具有 IP 网络上的所有安全风险，同时还面临无线信道安全风险，例如：空中泄露、IP 头通信流分析、WLAN 信号欺骗、WLAN 干扰、拒绝服务等；此外，WLAN 还面临一个特别的安全风险，即信息实际检测范围比通信范围大，攻击者可在其通信范围之外窃听到该网络上传输的数据。

无线局域网的网络环境安全需求主要包括：

（1）安全的接入网关或接入机制。

（2）对消息的强加密和通信流（包括头信息）安全有明确要求。

(3) 在局域网内,能够通过无线接入点以足够高的数据通信速率与有线网络进行通信,防止拥塞。

(4) 能够在网络上的各移动元素之间进行近范围的通信。

(5) 能够尽可能减小针对无线传输特征的识别行为。

无线局域网用户和移动终端的安全需求主要包括:

(1) 具有针对特定受限区域的访问控制机制。

(2) 具有针对用户和移动终端的标识与鉴别机制。

(3) 为确保数据机密性,用户和移动终端的软件应该与无线局域网中的软件保持兼容。

(4) 为保证无线局域网上终端的标识与鉴别、通信的机密性与完整性,建议在无线局域网的终端中采取端到端的 VPN 解决方法。

3) 微波与卫星通信

微波通信的安全需求主要是确保数据的机密性。通常可以采用在复接器(例如,路由器)、数字图像设备等各种终端与信道传输设备之间配置高速信道密码机的方式实现。

卫星通信网可由 TES 语音系统、ISBN/PES 数据网络传输系统、UMOD 点对点/点对数据传输系统组成,支持语音、数据、图像等各种信息的传输。在卫星通信中,在下行链路传输处窃听数据的行为可以在卫星覆盖区的任意地方完成,同时,卫星通信也容易遭受以电子干扰方式进行的拒绝服务攻击。

卫星数据通信的安全需求主要包括:

(1) 链路传输的安全性(主要是机密性和完整性)。

(2) 采取适当强度的网络边界防护措施。

移动卫星用户系统由用户环境、服务提供商网络和公共网络组成。可以在近期或不远的将来得到部分使用的这类卫星服务计划只有两个,即铱星系统和全球星系统。移动卫星系统的信息传输安全需求主要包括:

(1) 信息传输的连续性。

(2) 准确和及时的地理位置定位能力。

(3) 针对用户和接收方的标识与鉴别机制。

(4) 语音和数据的机密性、数据的完整性。

2 网络边界防护安全需求

网络边界防护用于限制外部非授权用户对内部网络的访问,通常由防火墙、接入安全控制设备和安全网关等网络安全设备共同提供。只要网络相互连接,就应该实施网络边界防护策略。一般地,该策略必须与信息敏感性、不同敏感性级别之间的差异、威胁和操作环境等因素保持一致。

1）通用安全需求

网络边界防护的通用安全需求主要包括：

(1) 为保证边界内部网络用户与所期望的外部用户或系统进行通信，网络边界防护策略不应该强迫用户使用任何非标准的协议或不规范的操作模式，不应该使用任何可能限制互操作性的流程。

(2) 对信息源、目的地和服务进行限制，阻断危险的协议（例如 ICMP 协议）。

(3) 对进入和越出网络边界的通信都进行限制。

(4) 限制可执行代码的服务和下载能力。

(5) 对网络边界的外来访问者，应用标识和鉴别机制（包括使用软件和硬件令牌）。

(6) 在适当的时候使用访问控制列表。

(7) 为防止未授权实体更改有关规则，应该采用认证机制。

(8) 为防止攻击者截获能够进行网络访问并获得访问控制权限的数据，采用加密技术（包括对远程管理的数据进行加密）。

(9) 为防范潜在的攻击行为，采用网络地址转换机制隐藏有关边界内部网络的地址和拓扑结构的信息。

(10) 对恶意软件进行扫描和监控。

(11) 记录和分析源路径与其他信息包，对攻击行为做出反应并进行限制。

(12) 操作者能够方便和正确地实施网络边界保护机制。

(13) 具备自监控和告警能力。

由于上述需求需要具体落实到不同的网络安全设备上，而这些设备的功能又各自不同，所以其安全需求又各自有别。网络边界防护对于这些网络安全设备的要求也不一样。下面以防火墙、安全网关、安全路由器、远程访问为例进行说明。

2）对防火墙的需求

防火墙的作用是防止位于网络内部的信息系统遭受外部的攻击（包括未经授权侵入系统、修改或删除数据、使用网络资源或服务，以及拒绝服务等），并支持内部的用户使用安全连接、并对边界内部的数据传输与存储提供保护。

网络边界防护需求对防火墙的要求是：

(1) 防火墙自身应该能够防渗透，因此应该建立在可信操作系统（可以是删除了不必要的可执行代码、编码器和其他不安全文件的操作系统简缩版本）之上，或者采用强制执行机制或者类似的机制。

(2) 应该支持对网络访问接入点的保护，这种保护对用户、相关组件和网络性能的影响应该尽可能地小，应该针对未来的需要具有可扩展性。

(3) 能够防止攻击者窃取有关防火墙配置规则、介质访问控制和其他控制信息。

(4) 能够防范各种网络攻击，确认攻击的来源和类型，对攻击做出反应，并对攻击造成的破坏进行恢复。

(5) 可信用户接入前必须通过智能卡、令牌等方法获得认证。

(6) 在需要加解密的时候，必须遵循统一的加密和密钥管理标准，采用具有兼容性的加密系统，以便不同厂商的防火墙之间能够进行通信。

(7) 防火墙组件的配置必须合理。

(8) 防火墙应该充分利用各种自监视工具，以便提供必要的访问控制机制，加强审计能力，并实施针对防火墙文件系统的整体检测。

3) 对安全网关的需求

安全网关依据网络的安全策略对进出网络边界的信息流进行控制和必要的处理。网络边界防护需求对安全网关的要求是：

(1) 自身应该能够防渗透，因此应该建立在可信平台(可以是删除了不必要的可执行代码、编码器和其他不安全文件的操作系统简缩版本)之上，或者采用强制执行机制(或者类似的机制)。

(2) 应该支持对于报文构造的验证，包括对可配置的报文的内容进行验证。

(3) 应该支持采用基于规则和密级由高到低的方式，对报文内容进行修改。

(4) 应该确保报文的安全级别不低于报文中附件的安全级别。

(5) 应该能够在报文通过时剥离其中的数字签名。

(6) 应该支持每个报文上的安全 ID 标记的可编程集合。

(7) 在连接两个具有不同密级的网络的情况下，安全网关应该支持在这两个网络之间合法的报文传输，同时也应该防止信息由高密级网络在未得到允许的情况下流向低密级网络。

(8) 应该对成功通过或未能通过的报文进行记录。

4) 对安全路由器的要求

网络边界防护对于安全路由器的要求与路由安全和数据机密性都有关系。这些要求具体是：

(1) 支持相应的网络协议(例如，RIP 路由协议、SNMP 协议、X. 25 协议、Frame Relay 协议、TCP/IP 协议、PPP 协议、IEEE 802. 3 Ethernet 协议等)。

(2) 支持访问控制。

(3) 支持设置非法 IP 地址。

(4) 支持根据设定的 IP 地址范围所进行加密和解密操作。

5) 对远程访问的要求

远程访问支持移动用户和固定用户通过电话线(例如，拨号接入)或数据网络进行数

据访问。另外,它也支持用户通过移动接入等方式访问网络内部资源(包括飞地资源)。远程用户采用的连接技术通常涉及 PSTN、数字无线业务网、ISDN 等。这些网络不仅会增大远程访问的威胁,也会因此而对安全解决方案带来体系结构方面的制约。远程访问连接期间,远程用户所用设备与远程被访问设备被认为具有同样的安全级别。网络边界防护对于远程访问的要求是:

(1) 远程用户终端上的密码应用接口应该与本地的密码应用接口相似,以便支持远程用户访问该终端上的资源。

(2) 采用连续的强认证。

(3) 远程用户所用设备和远程被访问设备之间的全部信息流均应该具备机密性,远程用户所用设备与其所处网络(例如 Intranet)之间的数据流应该具备完整性。

(4) 远程用户所用的硬件和软件应该具备完整性。

(5) 远程用户应该知道安全特性被激活的时间,并且能够方便地识别出这种情况。

(6) 有关远程访问安全的解决方案应该对远程用户的正常操作产生尽可能小的影响,并且不需要任何特殊的培训。

(7) 当远程用户被分离时,远程设备应该是无密级的设备,即远程用户端和远程被访问端设备上的数据和有关操作都应该在不受远程用户控制时得到足够的保护,以防止非受权的数据泄露、数据修改或操作。

(8) 移动用户的安全功能套件不应该包括任何特别的设备。

3. 网络上的检测与响应安全需求

网络上的检测与响应安全需求具体体现在基于网络的入侵检测、漏洞扫描、恶意代码防范和与网络有关的应急响应等方面。

1) 入侵检测

基于网络的入侵检测系统执行检测的基础是比较用户的会话(命令)参数和攻击者所采用技术的特征。它只是简单地监视网络上的信息传输,通常不具备加/解密能力。基于网络的入侵检测系统的安全需求主要包括:

(1) 该系统应该能够进行自检测,防止未经授权的访问和修改,并在必要的情况下通知服务控制台。

(2) 如果该系统发生了崩溃现象(无论是意外事件还是恶意行为所致),它应该能够得以恢复,并在启动后恢复到原先的状态并继续此前未能完成的操作。

(3) 该系统具备合理的网络兼容性。

(4) 该系统能够升级攻击特征数据,使得当新的攻击出现以后,系统能很快检测到新的攻击方式。

(5) 该系统应该便于依据被检测系统的安全策略进行操作，并且应该适应被检测系统和用户行为的变化。

2) 漏洞扫描

基于网络的漏洞扫描在网络上对目标结点进行探测，检测网络组件(包括主机)在网络连接中可见的漏洞，并在此基础上识别网络安全方案中的漏洞。它需要获知网络边界内部所有相关组件的有关信息。基于网络的漏洞扫描的安全需求主要包括：

(1) 由于此类漏洞扫描器仅对其配置中设定的对象进行检测，它的配置和设置必须合理。

(2) 由于此类漏洞扫描器通常通过检查对象的属性或通过模拟攻击者的行为来进行检测，所以必须确定正确的扫描时间和扫描方式，以免造成类似实际攻击事件所造成的影响。

3) 恶意代码检测与防范

影响恶意代码检测与防范效果的关键因素是该类型产品对于恶意代码的定义(例如厂商是否及时更新恶意代码数据库)和产品的使用方式是否正确(例如是否及时升级)和方便。基于网络的恶意代码检测与防范的安全需求主要包括：

(1) 能够进行数据完整性检测。

(2) 从高度可信的来源获取或下载恶意代码检测与防范工具(软件或硬件)。

(3) 能够对网络上的数据包进行监测。

(4) 能够采用某种适当的方式对包括电子邮件、Web 通信、FTP 会话、加密消息或压缩文件在内的所有进出网络的数据进行检测。

(5) 能够以实时方式或按需进行恶意代码扫描。

(6) 能够定位恶意代码的来源和类型，并依据入侵轨迹(或者支持采用某个灾难恢复计划)重建系统。

(7) 对网络用户和网络上的相关组件产生尽可能小的影响。

(8) 能够支持服务器级别或控制台级别的隔离。

(9) 能够提供相应的基于网络的响应服务，向网络(或系统)管理员和用户(例如被检测出带有恶意代码的电子邮件的发送者与接收者)报警。

(10) 能够通过网络或者其他方式及时进行版本升级。

4) 应急响应

应急响应是网络边界防护中的重要内容，其安全需求主要包括：

(1) 有合理、快捷的隔离措施可供选用。

(2) 采用有效地技术保留网络遭受各种入侵的原始数据，以便进行必要的取证。

(3) 依据必要的容灾、备份和恢复机制，尽快恢复网络的正常运行。

224　数据安全

数据安全主要关注信息系统中存储、传输和处理等过程中的数据的安全性，其目的是实现数据的机密性、完整性、可控性、不可否认性，并进行数据备份和恢复。

1. 数据机密性

数据机密性指传输和存储的数据不被非法获取。其安全需求与数据所处的位置、类型、数量、价值有关，涉及加密和访问控制这两种安全机制，具体包括以下几项：

（1）数据加密。

（2）数据隔离。

（3）通信流加密（例如数据填充或地址隐藏）。

2 数据完整性

数据完整性指传输或存储的数据没有被非法修改（包括数据进入传输信道时的序列号改变或重放）、删除。其安全需求与数据所处的位置、类型、数量、价值有关，涉及访问控制、消息认证和数字签名等安全机制，具体包括以下几项：

（1）防止未授权修改数据。

（2）对非授权数据修改的情况进行检测并记入日志。

（3）与源认证机制相结合。

（4）与数据所处的网络协议层的相关要求相结合。

3. 数据可控性

数据可控性指数据的复制、传输流向、传输流量和传输方式与安全策略（尤其是安全域的划分策略和网络边界防护策略）一致。其安全需求与数据所处的位置、类型、数量、价值有关，涉及访问控制、数字签名、密钥恢复、网络管理等安全机制，具体包括以下几项：

（1）禁止在未经授权的情况下复制数据。

（2）防止数据非法由高密级安全域流向低密级安全域。

4. 数据的不可否认性

数据的不可否认性指在数据的传输过程中，参与该传输过程的通信实体不能拒绝承认其参与该次传输过程的行为。数据的不可否认性通常由应用层提供。其安全需求与数据所处的位置、类型、数量、价值，以及参与数据传输过程的实体有关，涉及数字签名、加密、数据源与目的认证等安全机制，具体包括以下几项：

（1）具有数据源认证证据的不可否认性向数据接收方提供有关数据发送方的身份和原始发送时间的信息。

(2) 具有发送证据的不可否认性向数据发送方提供证据,证明数据被预订的接收方接收(某些情况下也包括证明接收时间)。

(3) 有可供采用的审计服务,提供对于涉及数据传输的各方的可审计性。

(4) 在高级别的安全保障环境中,应该采用可信时间戳记录通信发生的时间,并对数据和时间戳一同进行数字签名。

5. 数据备份和恢复

通过对数据采取不同的备份方式、备份形式等,保证系统重要数据在发生破坏后能够恢复。其安全需求类似于系统安全中的备份和恢复,整个信息系统需要通盘考虑。

225 应用安全

应用安全主要保障信息系统的各种业务应用程序安全运行,其安全需求主要涉及口令机制和关键业务系统的对外接口,包括电子邮件、文件传输、语音通信、视频会议与视频点播、Web 网站等。它主要与加密、数字签名、访问控制、认证、密钥恢复、网络监控管理和行政管理等安全措施有关。一般地,应从身份鉴别、安全标记、访问控制、可信路径、安全审计、剩余信息保护、通信完整性、通信机密性、不可否认性、软件容错、资源控制等方面考虑应用安全需求。下面将从一些典型业务应用程序的角度介绍应用安全的需求。

(1) 电子邮件的安全需求主要包括:对电子邮件用户进行基于数字证书的身份认证;支持基于 PKI 技术的邮件加解密、签名及其验证、时间戳等安全操作;支持安全电子邮件的收发和群发;能够通过与电子业务客户端的软件进行集成,完成个性化的安全操作。

(2) 文件传输是信息共享的基础,具体涉及三个过程,即消息处理、消息队列管理和审计管理。其安全需求主要包括:对文件的发送方与接收方进行身份认证;确保文件在其传输过程中的完整性(例如可采用数字签名、封装与解析等方法);能够记录系统运行步骤的出错信息,通过系统提供的管理工具查看日志。

(3) 语音通信的安全需求主要包括:防止包窃听/呼叫截获;进行身份认证和有效消除非授权访问,采用向管理员通报未知设备的方式防止呼叫者身份欺诈,采用禁止呼叫处理管理器配置未知电话和访问控制仅允许已知电话网相互通信的方式防止话费欺诈;通过呼叫处理管理器的呼叫设置记录提供防否认功能;防止 IP 欺诈(例如,在传输层交换机和状态防火墙上提供符合 RFC 2827 和 RFC 1918 技术要求的过滤器);为操作系统、设备和应用提供最新的安全修复,以便防范应用层攻击;防范拒绝服务(例如,将语音和数据网分开能够显著减少受拒绝攻击的可能性);通过采用有限信任模式和专用虚拟专用网(VLAN)信任关系,预防基于信任关系的攻击。

(4) 视频会议与视频点播的安全需求主要包括:对视频会议的用户进行身份认证,能够提供视频、音频处理与密码服务的接口,采用安全的计费系统,对视频点播文件采用

加密传输。

(5) Web 网站为接入用户提供统一的访问窗口和相关业务服务系统的连接。其安全需求主要包括：为发布在 Web 服务器和应用服务器上的信息提供防篡改服务，确保所发布的信息的正确性和完整性；具有针对 Web 访问流量的负载均衡功能，以便确保整个 Web 门户系统服务的可用性；提供与接入认证网关的接口，并且采用自主开发的安全通信协议，以确保各接口的安全性与稳定性；在节约成本的情况下，为提高系统的可靠性，Web 服务器应该互为备份。

226　安全管理

信息系统的生命周期主要包括五个阶段：初始阶段、采购/开发阶段、实施阶段、运行维护阶段、废弃阶段。针对这五个阶段，下面将从安全管理制度、安全管理机构、人员安全管理、系统建设管理和系统运行维护管理等方面考虑其安全需求。

(1) 安全管理制度，主要从管理制度、制定和发布、评审和修订三个方面分析和确定其安全需求。

(2) 安全管理机构，主要从岗位设置、人员配备、授权和审批、沟通和合作以及审核和检查五个方面分析和确定其安全需求。

(3) 人员安全管理，主要从人员录用、人员离岗、人员考核、安全意识教育和培训以及外部人员访问管理五个方面分析和确定其安全需求。

(4) 系统建设管理，主要从系统定级、安全方案设计、产品采购和使用、自行软件开发、外包软件开发、工程实施、测试验收、系统交付、系统备案、等级测评和安全服务商选择十一个方面分析和确定其安全需求。

(5) 系统运行维护管理，主要从环境管理、资产管理、介质管理、设备管理、监控管理和安全管理中心、网络安全管理、系统安全管理、恶意代码防范管理、密码和密钥管理、变更管理、备份和恢复管理、安全事件处置、应急预案管理十三个方面分析和确定其安全需求。

2.3　信息安全体系结构的设计目标、指导思想与设计原则

231　设计目标

随着各行各业信息化程度的深入，信息技术的应用已经与办公方式、业务运行产生了千丝万缕的联系。这就使信息安全体系结构的设计不再是一件仅仅能够由信息安全专业

人员自行完成的简单工作，而是需要得到用户的密切协作。

设计信息安全体系结构的目标是帮助采用该体系结构的用户满足其信息安全需求，从而对其相关资产进行保护。在这里，“用户”可以是任何具有信息安全需求的组织机构（包括企业）的整体或部分，也可以是具有信息安全需求的个人。

对于组织机构而言，在没有接受专业化的信息安全技术与管理服务之前，其信息安全需求可能会呈现出复杂多样、难于表述的状况。即使前期有过一些相关的体验，一旦融进新的业务，面临新的隐患，或者了解到也许可用的新技术，信息安全需求都会相应地发生变化。在这种情况下，为了对组织机构的相关资产保护到位，信息安全体系结构的设计人员就必须身临其境，帮助对方理清各项重要的资产，发掘他们真实、客观的信息安全需求，在进行充分讨论并得到对方确认之后，提供解决方案。这时，“方案”可能会较多地涉及对方的管理方式和流程，或者更多地侧重于提供一种技术实施方法。

对于个人用户而言，需求相对会明确得多，其中以保护重要数据的机密性、保障网络与数据的可用性为重点。相应地，“方案”会比较偏向于实现一种或多种信息安全技术。

2.3.2 指导思想

设计信息安全体系结构的指导思想是：遵从国家有关信息安全的政策、法令和法规，根据业务应用的实际需要，结合信息安全技术与产品的研究与开发现状、近期的发展目标和未来的发展趋势，吸取国内外的先进经验和成熟技术，采用科学的设计方法，力争在设计中融入具有自主知识产权的技术与产品，鼓励技术与产品创新。

2.3.3 设计原则

信息安全体系结构的设计必须贯彻信息系统安全工程的思想，并遵循以下六项基本原则。

1. 原则一——需求明确

明确业务系统的信息化需求，明确信息系统建设的信息安全需求，以及拟采用的主要信息安全技术与产品的应用需求。

2. 原则二——代价平衡

对可能面临的安全风险进行定性与定量的评估，在安全需求、安全风险和成本之间进行综合考虑和仔细权衡，制定相应的规范和措施，确定实际可行的安全策略，在确保将信息安全风险控制在可接受范围内的前提下，将信息安全体系结构的整体成本控制在合理范围之内。

3. 原则三——标准优先

在信息安全体系结构设计的过程中积极采纳现有的技术标准和管理标准，以求该设计具有横向、纵向的连通性，节约后期的建设成本；对于国际标准和国家标准的采用，应理解相关的国际动态，明确有关的国家政策，力所能及地鼓励自主标准的开发与推广。在标准化方面，总的原则是遵循国家标准，兼顾国际标准。在国家标准不同于国际标准的情况下，要遵循国家标准，在国家标准要求低于国际标准的情况下，要尽量遵循国际标准。

4. 原则四——技术成熟

在信息安全体系结构设计的过程中采用成熟的信息安全技术与产品，同时关注这些技术与产品的发展态势。对于新出现的功能复杂的技术与产品，除非特别需要，并且进行过充分论证，方可采用。

5. 原则五——管理跟进

结合技术产品的应用情况和人员素质情况，制定必要的管理措施，包括各种与信息安全管理相关的规章制度、必要的培训与考核制度，并且对这些措施的具体落实情况进行定期追踪和不断改进。

6. 原则六——综合防护

从一个完整的安全体系结构出发，综合考虑信息网络的各种实体和各个环节，综合使用针对不同层次的不同安全手段，关注整体安全而非局部效应。由于设计中采用的各种技术与产品种类繁多，结构复杂，如果采用单一的防护措施，即使每一项安全措施可以起到它应有的作用，综合起来也不一定能达到应有的效果。只有采用多种安全措施，按照纵深防御的战略，分层次、有重点地对目标加以防护，才能达到要求的安全目标。相反地，采取简单、零散的防护措施，不仅有可能造成资源浪费，更重要的是，极有可能达不到要求的安全目标。另外，我们不仅要注重防外，也要注重防内，防外与防内并重。

2.4　安全策略的制定与实施

2.4.1　安全策略

安全策略是用一般的术语对安全需求和属性进行描述，不涉及具体的实现过程。安全策略涉及的因素很多，主要包括硬件、软件、访问、用户、连接、网络、电信以及实施过程等。安全策略的作用是表现管理层的意志、指导体系结构的规划与设计、指导相关产品的选择和系统开发过程、保证应用系统安全的一致性和完整性、避免资源浪费，以及尽可能

消减安全隐患。

2.4.2 制定依据

制定安全策略首先需要综合考虑上述六项基本设计原则，但也需要针对具体的对象。这些对象可以是一个设备（例如，路由器、防火墙），可以是一个网络区域（例如，局域网、Internet），也可以是某种安全机制（例如，访问控制、物理安全）。例如，可以针对电子邮件系统的使用制定电子邮件安全策略，也可以针对某个重要机房的访问制定机房物理访问控制安全策略等。

此外，安全策略的制定必须确保其可实施性。即使对于非专业人员，看到了安全策略，也能够明白自己需要怎么做，才能够不违反这些安全策略。那些虽然表述得很清楚，外行看来也很容易看懂，但是没有办法具体执行的所谓安全策略，并不具有实际的作用。

2.4.3 安全策略分类

一般地，可以将安全策略分为管理性安全策略和技术性安全策略。

1. 管理性安全策略

管理性安全策略主要涉及内部人员安全策略，物理和环境安全策略，应用操作中的输入输出介质控制策略，应急策略，硬件和系统软件维护控制策略，完整性控制策略，归档策略，安全意识和培训策略，事件响应策略等。下面分别介绍这些管理性安全策略需要考虑的要素。

1）内部人员安全策略

内部人员安全策略需要考虑以下内容：

（1）确定所有相关工作职位的人员密级要求。如果该要求尚不明确，应制定相应工作日程。

（2）对各职位上的工作人员进行必要的背景调查。如果调查结果尚不明确，制定相应的调查日程。若在调查不充分的情况下，某个职员获得授权进行网络或系统操作，需要记录有关情况并考虑必要的风险应对措施。

（3）采用最小特权策略，将人员的操作权限限制在最小可能的权限范围内。

（4）对关键操作的权限进行分割，使该权限分散在若干不同操作人员中，以免某个（或某些）人员获得可能进行欺诈所需的全部授权和所有信息。

（5）确定一个有效地管理过程，对用户的口令账号进行查询、建立、授权和撤销。

（6）确定必要的监督和审核机制，促使有关人员对其各自的行为负责。

（7）结合具体职位的安全意识和安全技能需求，对内部人员进行相关培训，尽可能减

少误操作。对于与外界交往或通信频繁的内部人员，尤其要注意提高其安全意识，防止他们无意识地泄密。

(8) 确定雇佣合同的终止方式(包括友好的方式和非友好的方式)。

2) 物理和环境安全策略

物理和环境安全策略需要考虑以下内容：

(1) 访问控制措施(例如，采用门禁系统、生物识别装置、红外摄像装置等)。

(2) 结合具体的物理和环境安全需求，制定严格的、可操作的外来人员访问记录规章，并指派专人定期进行审核。

(3) 防火措施。

(4) 操作环境安全措施(例如，供电系统、空调系统等的安全部署)。

(5) 建筑物的抗震性能(与地震等灾害有关)、承载性能(与雪灾等灾害有关)、抗毁性能(与管道爆炸等灾害有关)。

(6) 管道防泄露措施。

(7) 数据窃取防范措施(例如，防止偷窥、侦听和电磁泄露等)。

(8) 对于移动和便携设备的物理安全和数据安全防范措施。例如：安全存放笔记本计算机，对移动和便携设备中的数据及时进行备份。

3) 应用操作中的输入输出介质控制策略

应用操作中的输入输出介质控制策略需要考虑以下内容：

(1) 获得内部人员和外界相关人员(例如，软件送货商)的支持，必要的情况下可以通过签订合同加以约束。

(2) 采用适当的密级标记(显式标记或隐式标记)。如果是采用显式密级标记，必须确定与之相对应的要素(例如，日志/目录标识，受控访问，特殊存储措施，发布或销毁日期等)。

(3) 确定用户无法对输入输出介质进行任何非授权的操作。

(4) 对于达到敏感级别的输入输出介质的接收，必须进行审计追踪。

(5) 对输出介质采取访问控制措施。

(6) 对以传统方式传输或邮寄的介质或书面材料，采取访问控制措施。

(7) 针对目录管理，确定审计追踪机制。

(8) 对于存储介质的物理和环境，确定相应的保护措施。

(9) 对于电子存储介质的信息，确定其擦除和介质重用措施(例如，写覆盖或消磁)。

(10) 对于无法有效擦除并重用的、受损的受控存储介质，确定相应的处理措施。

(11) 对于印刷材料，确定采用安全的销毁措施。

4）应急策略

应急策略需要考虑以下内容：

（1）部署有效的、经过验证（或论证）的应急计划，以便在灾难发生的情况下支持关键系统的连续性。

（2）确定完善的备份机制。

（3）为所有的网络和信息系统制定有效的、经过验证（或论证）的灾难恢复计划。

（4）张贴或采用其他公告方式，发布正式的、书面的应急操作计划，以便提高该计划的易用性。

（5）对应急计划的实施状况和合理性进行周期性地检验。

（6）对所有相关人员进行应急计划相关培训。

（7）在需要获得外界人员支援的情况下，确定可能存在的安全隐患，并制定相应的监督和防范机制。

5）硬件和系统软件维护控制策略

硬件和系统软件维护控制策略需要考虑以下内容：

（1）与外连网络（或设备）的所有者签订硬件和系统软件维护合同。

（2）确定需要进行硬件和软件维护控制的原因。如果是由与其相连的外界网络（或设备）导致，则与该网络（或设备）的所有者联系，协商具体的解决办法。

（3）硬件和软件的维护过程可能对网络和系统安全造成影响。确定影响的程度，以及减少这种影响的具体措施，例如：限制硬件和软件维护人员的身份和权限；在应急状况下，采取特殊的硬件和软件维护过程；对硬件和软件的授权和升级进行管理，合理使用这些管理权限，并尽可能地降低维护成本；确定以在线和离线方式进行的硬件和软件维护过程的安全（例如，为维护人员配备陪同人员，安全地处理离线设备等）；确定远程维护过程中的设备维护和控制措施。

（4）确定系统的配置管理过程，具体包括：进行版本控制，并且依据需要及时进行版本更新；依据网络和系统的变化情况，及时更新应急计划和相关文档；确保测试数据的实时性；制定和及时采用应急处理措施。

6）完整性控制策略

完整性控制策略需要考虑以下内容：

（1）安装病毒检测和消除软件，及时恢复受病毒感染的文件，采用自动或手动方式进行病毒扫描，确定病毒查杀步骤和病毒报告机制。

（2）采用必要的完整性校验机制（例如，校验和、Hash 值等）。

（3）采用口令校验机制。

（4）采用监控技术，对网络和系统运行期间的日志进行实时分析，及时发现可能影响

或破坏可用性的潜在问题(例如,主动攻击、运行异常或崩溃等)。

(5) 在应用层上,采用消息认证机制,确保消息被正确的接收者接收,以及消息在传递过程中没有被篡改。

7) 归档策略

归档策略需要考虑以下内容:

(1) 软件与硬件提供商提供的有关文档。

(2) 安全策略文档。

(3) 测试文档。

(4) 标准的操作说明文档。

(5) 应急处理操作文档。

(6) 应急计划文档。

(7) 灾难恢复操作文档。

(8) 风险评估文档。

(9) 备份操作文档。

(10) 与外连网络(或设备)所有者签订的硬件和系统软件维护控制合同文档。

(11) 对上述文档的授权处理方式。

8) 安全意识和培训策略

安全意识和培训策略需要考虑以下内容:

(1) 确定进行安全意识培训的材料。

(2) 针对不同的用户,确定周期性的培训计划和实施方式。

(3) 确定针对培训结果的考核措施。

9) 事件响应策略

事件响应策略需要考虑以下内容:

(1) 确定事件响应有关信息(例如,软件补丁、系统脆弱性)的接收者和响应者。

(2) 确定采取的防范措施,包括:入侵检测工具、自动化的审计日志、渗透测试等。

(3) 确定在必要的情况下需要求助的外部资源(例如,某个专业机构),以及发布求助信息的过程。

2 技术性安全策略

技术性安全策略主要涉及标识和认证策略、逻辑访问控制(授权/访问控制)策略、公共访问控制策略、审计追踪策略等。下面分别介绍这些技术性安全策略需要考虑的要素。

1) 标识和认证策略

标识和认证策略需要考虑以下内容:

(1) 采用唯一标识符(ID)进行标识。

(2) 标识应该与用户的行为相关,并且具有明确的有效期。

(3) 对用户 ID 进行及时更新和定期维护。

(4) 确定用户认证机制(口令、令牌或生物认证机制)。

(5) 如果是采用口令系统,则应该提供以下信息:可用的字符集、口令长度的最大值和最小值、口令有效期和更新方法、针对口令丢失的相应处理办法、针对口令篡改的相应处理办法。

(6) 进行用户培训。

(7) 确定所需采用的生物识别技术及其实现方式,具体包括:是否需要特殊硬件读取设备;是否要求用户使用一个特定的个人标识号(PIN);PIN 的确定方法(用户选择或系统管理员指定);是否需要采用口令产生器或一次性口令;若采用一次性口令,是否需要采用应答机制。

(8) 确定访问控制机制的实现位置(网络层、操作系统层或应用层)。

(9) 确定访问控制机制对可审计性和审计追踪机制的支持方式(如口令与用户标识符相关)。

(10) 确定用户识别机制所需的自保护技术(例如,对传输和存储的口令进行加密,自动生成口令,依据禁用口令列表对口令的有效性进行检验)。

(11) 确定允许来自给定用户标识符或访问主体(终端或端口)的无效访问最大次数,并确定相应的处理方式。

(12) 更改系统提供的默认口令,并确定针对这种更改的验证措施。

(13) 确定针对带有内置口令的脚本的访问限制措施(例如,禁止使用或仅在批处理的情况下允许使用)。

(14) 确定所有无须遵从用户识别要求的安全策略、单点登录技术有关信息(例如,主机-主机标识符,识别服务器标识符,用户-主机标识符,组标识符)、其他弥补性的控制措施。

(15) 若采用数字签名技术,该技术必须遵循有关的权威性技术标准。具体需要考虑的内容是:确定所采用的数字签名标准(包括依据要求提供使用期限、授权方身份信息);确定数字签名或其他可供使用的安全控制方法的实现方式;确定密钥管理措施。

2) 逻辑访问控制策略

逻辑访问控制又称授权/访问控制,其策略需要考虑以下内容:

(1) 针对每个用户或每类用户,明确正式的授权策略,指明该授权是否遵循最小特权策略。

(2) 为防止用户获得进行欺诈活动所需的全部授权和所有信息，逻辑访问控制策略必须对用户的职责进行分割。

(3) 采用访问控制列表，并确定是否需要以手工方式维护访问控制列表。

(4) 确定安全功能软件使用者的授权权限，即这些使用者是否能够限定其他用户(包括一般用户、系统管理员或操作员等)对应用程序、数据或文件的访问权限。

(5) 确定应用层用户对超越其使用范围的操作系统、其他应用或系统资源的访问权限。

(6) 及时更新和定期维护访问控制列表。

(7) 依据具体应用要求，确定是否需要采取强制访问策略；对于所有相关证明的评价信息进行归档。

(8) 采取必要的控制措施，检测授权用户和非授权用户的越权使用行为。

(9) 确定用户休眠时间的上限，以及系统在此情况下的应对措施(如要求重新输入口令、显示黑屏等)。

(10) 严格限制用户在正常工作时间之外的系统访问。

(11) 对于敏感信息的非授权访问，确定是否需要采用密码机制进行限制(不包括以认证为主要目的而采用的密码机制)。在需要采用密码机制的情况下，必须提供以下相关信息：采用的密码方法(包括有关密码产品和标准)，采用的密钥管理方法。

(12) 在网络边界或系统上应用必要的安全措施，包括硬件和软件控制措施，防止非授权系统的渗入和其他网络的威胁与脆弱性。

(13) 明确所用安全网关或防火墙的类型、功能和配置要求。

(14) 对于针对通信端口的特殊访问，要求提供该端口保护设备的相关信息，包括端口保护设备的配置信息、必需的口令或令牌信息等。

(15) 在对访问特定信息类型或文件进行控制的情况下，确定是否需要采用内部安全标签，以及该标签是否要求采用某种特定的保护措施或处理规则。

(16) 明确是否需要采用基于主机的认证机制。

3) 公共访问控制策略

公共访问控制策略需要考虑以下内容：

(1) 采用某种形式的标识和认证机制。

(2) 对用户的读、写、修改或删除等操作进行授权控制。

(3) 防止公共用户修改系统信息。

(4) 采用数字签名技术。

(5) 采用 CD-ROM 方式发布在线存储的信息。

(6) 对公共访问信息进行备份。

(7) 禁止对实时更新的数据库进行公共访问。

(8) 对向公众发布的程序和信息进行验证,以防病毒利用这些程序和信息进行传播。

(9) 确保审计追踪信息和用户信息的机密性。

(10) 确保系统和数据的可用性。

(11) 遵从相关法律法规。

4) 审计追踪策略

审计追踪策略需要考虑以下内容:

(1) 使用在线审计追踪工具,识别除入侵之外的类似问题。

(2) 使用采用审计追踪工具,判断这类事件的发生时间、来源和原因所需要的足够的信息,事件记录的具体内容通常包括:事件类型、事件发生时间、与该事件相关的用户ID、触发该事件的程序或命令。

(3) 对于在线访问审计日志的请求和行为进行严格控制。

(4) 确保访问控制功能管理员和审计追踪管理员具有各自不同的职责。

(5) 确保审计追踪信息的机密性。

(6) 确定审计追踪的执行指南,对审计追踪的执行情况进行周期性检查。

(7) 确定审计追踪信息的查询方式。

(8) 支持正确的系统层面或应用层面的管理员依据确定的系统故障或应用故障,或者依据确定的违反相关要求的事件,对审计追踪策略进行检查。

(9) 以实时或接近实时的方式应用审计分析工具(如基于审计规约、攻击签名和其他多种技术的审计分析工具)。

2.5 小结

本章重点介绍了四个内容:一是用实例分析了网络和信息系统的总体结构与安全之间的关系,并给出了信息系统的定义;二是从物理安全、系统安全、网络安全、数据安全、应用安全与安全管理六个层面比较详尽地分析了信息系统的安全需求;三是介绍了信息安全体系结构的设计目标、指导思想与设计原则;四是介绍了安全策略的作用、制定依据和分类。

信息系统是由计算机及其相关的和配套的设备、设施(含网络)构成的,按照一定的应用目标和规则对信息进行采集、加工、存储、传输、检索等处理的人机系统,也称计算机信息系统。保障信息系统安全的第一步就是对信息系统的体系结构进行分析,充分了解其架构和规模;其次,就是进行信息安全需求分析,本书从六个层面介绍了信息安全需求所

要分析的方方面面;再次,就是要确定信息安全策略和保障重点。本章内容是进行信息系统安全顶层设计的基础。

习 题

1. 简述网络体系结构与安全之间的关系,并叙述信息系统的基本内涵。

2. 画图说明物理安全、系统安全、网络安全、数据安全、应用安全与安全管理六个层面之间的逻辑关系。

3. 简述物理安全、系统安全、网络安全、数据安全、应用安全与安全管理六个层面的主要安全需求,并说明在一个信息系统中如何来平衡这些安全需求。

4. 比较系统安全需求与网络安全需求之间的异同点。

5. 谈谈自己对信息安全体系结构的设计原则的理解。

6. 什么是安全策略? 阐述安全策略的分类及其具体内容。

7. 论述安全需求与安全策略之间的关系。

8. 你认为应该从哪一个视角进行信息安全需求分析?

第3章 信息安全技术支撑

信息安全体系结构的设计和构建，需要多种信息安全技术的支撑。这些技术主要包括密码服务、密钥管理、认证、授权、容灾备份与故障恢复、恶意代码防范、入侵检测、安全接口与中间件、无线网络安全等。本章介绍这些技术的基本原理、主要作用、通用要求和体系结构。本章的内容与第4章的内容密切相关，相关内容之间可以相互补充。

相对而言，某些技术（例如，密码服务、密钥管理、恶意代码防范、入侵检测）较为成熟并已自成体系，市场上可供选择的产品也较多，可以结合应用需求独自加以应用；另一些技术（例如，认证、授权、容灾备份与故障恢复、安全接口与中间件、无线网络安全）则在实施过程中必须结合考虑其他技术的应用情况进行适当调整，以免由于采用了这些技术，占用了过多的系统资源或网络资源，或者增加了信息系统建设成本，给网络与信息系统的正常、有效运行带来不必要的负面影响。

3.1 密码服务技术

3.1.1 作用

密码服务技术为密码的有效应用提供技术支持。一般地，密码服务系统由密码芯片、密码模块、密码机或软件，以及密码服务接口构成。例如，为密钥管理基础设施提供加密服务的加密服务器、应用代理服务器的加密服务器及用户使用的智能卡。密码服务系统本身是密码、密钥和证书的重要载体，具备完善的安全防护措施和大容量的存储空间；密码设备的管理也是非常重要的，必须符合上层安全管理接口的规范要求，接受安全管理系统统一的监控。密码芯片及部分安全模块，由于嵌入到各种密码应用设备里，因此安全管理接口由上层系统提供。软件令牌由于作为开放的公众应用，不具备安全管理的接口。

通常，密码服务系统以独立的形式，提供各种安全服务，并具备完善的安全机制以及规范的编程接口。

3.1.2　要求

1. 安全要求

一般地，密码服务器及安全模块的设计应该满足以下的安全要求：

(1) 采用可信计算机。

(2) 具备设备安全和敏感信息保护机制。

(3) 关键设备的真实性鉴别。

(4) 具备完善的密钥管理机制。

(5) 符合工业标准。

(6) 提供日志审计及统计服务。

(7) 支持监测响应系统的统一监测。

(8) 支持安全管理系统的统一管理。

2 功能要求

为保证系统安全和信息的机密性、完整性、真实性和不可否认性，密码服务系统的主要功能要求如下：

(1) 密钥管理服务。

(2) 数字证书管理服务。

(3) 数字证书运算：提供数字证书签发和验证等基本的证书运算服务功能。

(4) 数据加解密运算：提供对数据的加密和解密等运算功能。

(5) 数字签名运算：提供对数据的签名和签名验证等运算功能。

(6) 数字信封：提供对数据的数字信封封装和解封装等运算功能。

(7) 消息摘要和完整性验证：提供对消息进行摘要运算功能，并具有验证消息完整性功能。其核心功能应该是提供加解密服务、密钥管理和证书管理，而其中的 PKI、KMI 等的密码服务器应能支持国家密码主管部门指定的密码算法。

3.1.3　组成

通常情况下，密码服务系统由密码芯片、密码模块、客户端密码服务设备、服务器端密码服务设备等组成。

1. 密码芯片

密码芯片包括 ASIC、FPGA 等载体作为密码运算单元，这类单元通常支持单一或组合的密码运算及密钥输入，具有专有的通信接口协议或口令等安全保护措施，并具备基本的自身防护机制，如不可被分析、密钥不可被读出。

密码芯片的功能要求必须符合相应的电器特性，以及硬件接口标准，包括数据总线、异步时序、同步时序、寄存器操作等接口标准。通过 RAM 传输模式、FIFO 传输模式提供数据的交互。

2 密码模块

密码模块专指具备完整安全功能及服务的加密卡、高度集成的安全芯片等，通常集成了密码运算单元、噪声源、密码协议、密钥管理等功能，能够提供一种或多种安全中间件下层密码服务接口接入。这类设备通常用于 VPN、链路密码机等各种密码服务设备，也可以直接作为客户端密码服务设备。

这类设备通常要求具有完善的自身防护机制，包括管理机制及销毁措施，并符合密钥管理、安全管理的要求。

3. 客户端密码服务设备

这类设备的作用是提供终端密码服务。它们具有便携式、功能齐全、成本低等特点，便于大规模使用以及移动办公。从其组成和功能上来看，它们通常具备通用的密码运算单元、密钥管理、用户证书管理、安全管理等部件，能够支持应用系统客户端的各项安全应用。

4. 服务器端密码服务设备

这类设备的作用是为密钥管理基础设施（KMI）、公开密钥基础设施（PKI）、安全管理设备、安全防护设备（例如，应用网关、接入认证设备、应用服务器）等，提供性能稳定、功能强大的安全服务设备。它们具备完善的自身防护、密钥管理、证书管理以及安全管理机制。这类设备可以提供多种密码服务系统接口，能够作为多个安全模块接入安全中间件，通常以 SOCKET 形式提供安全服务，与网络逻辑隔离。

3.1.4 密码的使用

密码服务系统所使用的安全模块或密码设备，均应严格按照国家相关主管部门的有关规定，采用经国家相关部门批准的核密、普密或商密产品。

在密码使用方面，各种密码服务系统提供不同的算法和协议支持，策略库根据国家密码主管部门要求来设置，用户可以在策略库的规定范围内，灵活地选择并配置合适的密码算法及其协议。对关键的密码服务系统，必须采用统一的安全管理策略。

一般地，一个实际的应用系统会涉及以下几个方面的密码应用：

（1）数字证书运算：提供对数字证书的产生、签发和验证运算。

（2）密钥加密运算：提供密钥的安全传输和存储的加解密运算。

（3）数据传输：提供数据安全传输的加密和解密运算。

（4）数据存储：提供数据安全存储的加密和解密运算。

（5）数字签名：提供对数据的签名和签名验证等运算。

（6）消息摘要与验证：提供对消息进行摘要运算及完整性验证运算。

（7）数字信封：提供对数据的数字信封封装和解封装等运算。

3.1.5　密钥的配用与管理

密钥的使用与管理涉及公钥密码体制的公钥、私钥，以及对称密码体制的秘密密钥。所有密钥都要遵循严格的配用原则，包括最小特权原则，特权分散原则，最小设备原则，不影响系统正常工作的原则。密钥管理涉及密钥生命周期的全过程。对不同的密钥类型采用不同的管理办法。

3.1.6　密码服务系统接口

密码服务系统接口（CPI）为密码服务相关的应用开发，提供标准化的安全接口平台，根据不同密码载体，其提供形式多种多样。CPI 属于安全接口体系的底层。CPI 有多种类型（参见 3.8 节），但是每一种都包含了几个共同的部分，即安全管理接口、密钥管理接口等，用以提供对该设备的管理服务。安全管理服务将由安全管理模块统一提供，密钥管理服务由密钥管理模块提供。

对于密码服务系统，所提供的接口必须符合上层安全中间件的接口规范，即 CPI 的规范要求，同时支持动态加载。安全中间件要求密码服务系统接入前必须通过相关功能测试，同时要求通过国家相关的检验，然后才可以对其提供的 CPI 进行签名。安全中间件加载设备前要验证其签名，并检验其完整性，确保其合法且没有被篡改过。

对于服务器密码机，根据类型不同，要求支持实时、多任务、面向连接和无连接等各种形式的高端应用，同时必须提供符合标准的安全管理及监控接口。

对于专用加密模块和芯片，则主要以各个厂商提供的产品接口规范为依据，直接提供给密码应用设备的设计生产厂商。由于与硬件时序直接相关，所采用的标准也可能各不相同，同时各自还具有自身的特点，不便于规范。但是，可以支持符合国际标准规范的安全模块接口，如 ISO 7816 等。

密码服务系统提供的 CPI 的主要任务是封装硬件接口驱动，包括各种操作系统平台、硬件平台的驱动，必须具备良好的性能和兼容性。同时提供基本密码函数、密钥管理接口调用，安全协议及模型则交由上层中间件进行封装。这其中包括 RSA、DSA、ECC 公钥密码函数接口及 DES、3DES 及 HASH 函数，国家自主知识产权的密码函数接口以及基本的管理接口等。

密码服务系统接口主要以标准 C/C++/C# 提供。

3.2 密钥管理技术

3.2.1 作用

密钥管理技术的作用是为应用系统提供集中和统一的密钥支持和密钥管理服务。这类服务通常由密钥管理基础设施(KMI)来提供。主要包括用户注册、密钥下载、密钥管理、密钥协商、系统日志和审计等功能。

1. 用户注册功能

通过离线方式,由核心区注册终端录入密码机实体相关信息、加密设备的用户相关信息。

2. 密钥下载功能

依据用户要求,采用 Web 方式下载证书。

3. 密钥管理功能

为单个加密设备或一组加密设备进行密钥生命周期中的所有操作。具体内容包括以下几点:

(1) 密钥生成与装载:通过对密钥机和用户信息的变换生成密钥,并通过一个安全的密钥注入方式为密码机装载这些密钥。

(2) 密钥分发:以安全的方式将密钥从产生器分发到用户设备,可以采用公钥技术在产生器和用户设备之间传送对称密钥,或者通过允许用户设备产生一个授权的会话密钥的方式在密钥产生器与用户设备之间传送对称密钥。

(3) 密钥存储:以加密形式存储密钥,严格控制存储期,采取必要的安全机制限制对这些密钥的访问。

(4) 密钥销毁:安全地销毁不再使用的密钥。

(5) 密钥更新:先销毁待更新的密钥,再通过密钥的生成、装载、分发、存储等步骤产生一个新的密钥。

4. 密钥协商功能

在各级安全管理中心之间,建立信任关系,实现相同或不同密钥管理域密码终端之间的密钥协商,满足跨管理域的加密通信。

5. 系统日志和审计功能

采用附加机制对密钥的整个生命周期进行跟踪,以定时或实时的方式对管理对象的

密钥、重要操作、安全事件等信息进行审计。KMI 的审计终端将记录获授权人员对 KMI 的访问时间、被访问密钥属主信息、要求进行的操作记录等信息，保存相应的签名记录和证据。系统还提供记录操作员的所有操作活动及与 KMI 的交互活动的时间、事件等信息。

3.2.2 体系结构

KMI 的体系结构通常采用树状结构，各结点均设置密钥管理系统，相邻层的结点之间采用加密通信的方式进行密钥传输和管理信息传输。

密钥管理系统由密钥管理服务器、管理终端、数据库服务器、密码服务系统等组成。其中，密钥管理服务器为密钥的整个生命周期提供完善的管理服务。密钥管理系统的组成如图 3-2-1 所示。

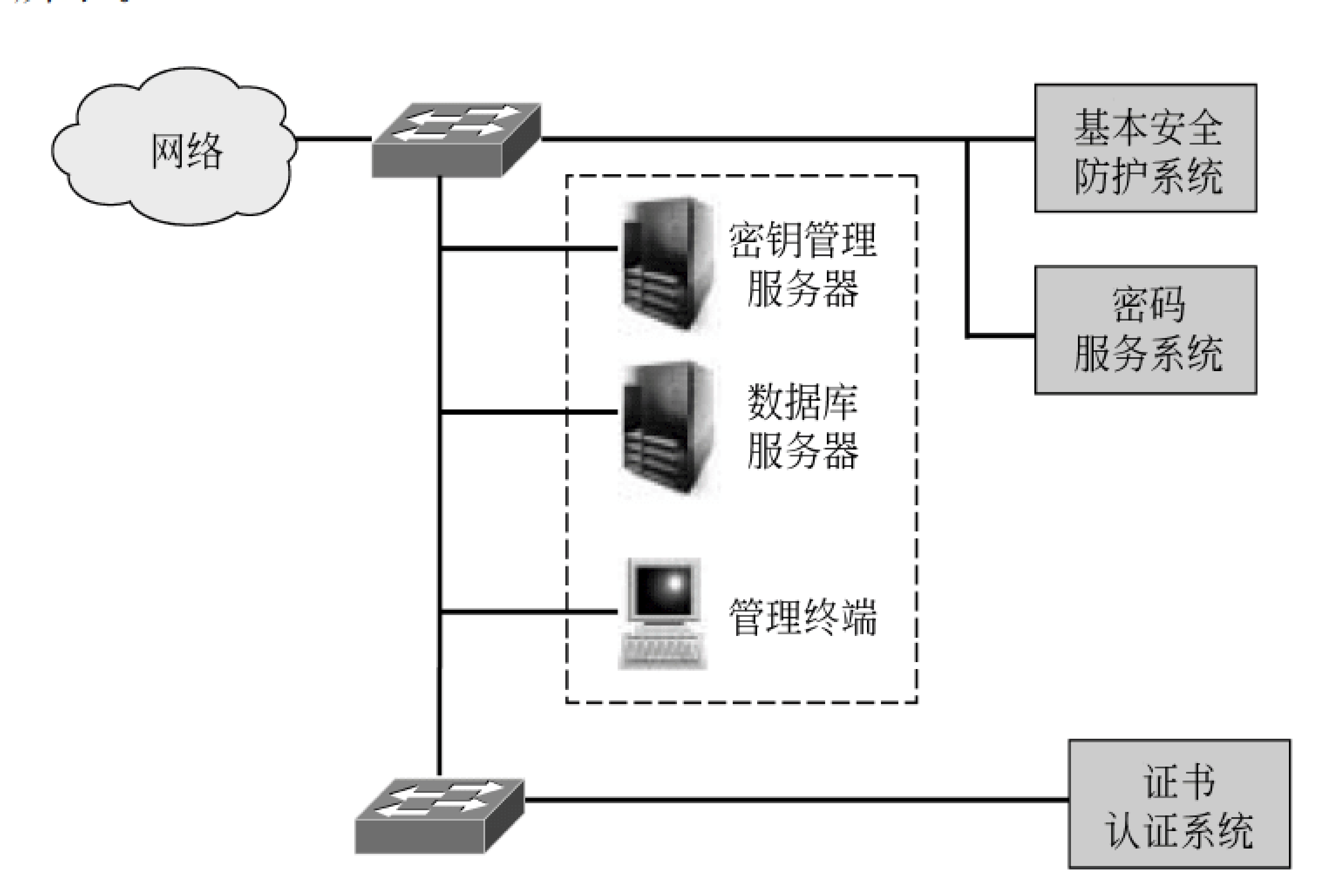


图 3-2-1 密钥管理系统组成

从逻辑上来看，密钥管理系统又由密钥生成子系统、密钥库子系统、密钥恢复子系统、密钥管理子系统和管理终端组成，其逻辑结构如图 3-2-2 所示。

(1) 密钥生成子系统：与密码服务系统相连，负责密钥对的生成，由随机数发生器产生真随机数作为种子，在服务器上运行特定的算法，生成密钥对，验证密钥对的安全性，若是安全的，则确定为所需的安全密钥对。

(2) 密钥库子系统：用于存放密钥，包括预生成、已使用和归档库三个库。预生成库存储了还没有生成用户证书的用户密钥对；已使用库存储了正在使用证书对应的密钥对；当用户进行更新、注销操作后，其密钥对则转入归档库。

(3) 密钥恢复子系统：为用户提供密钥恢复功能。用户发生加密密钥损坏、遗漏等

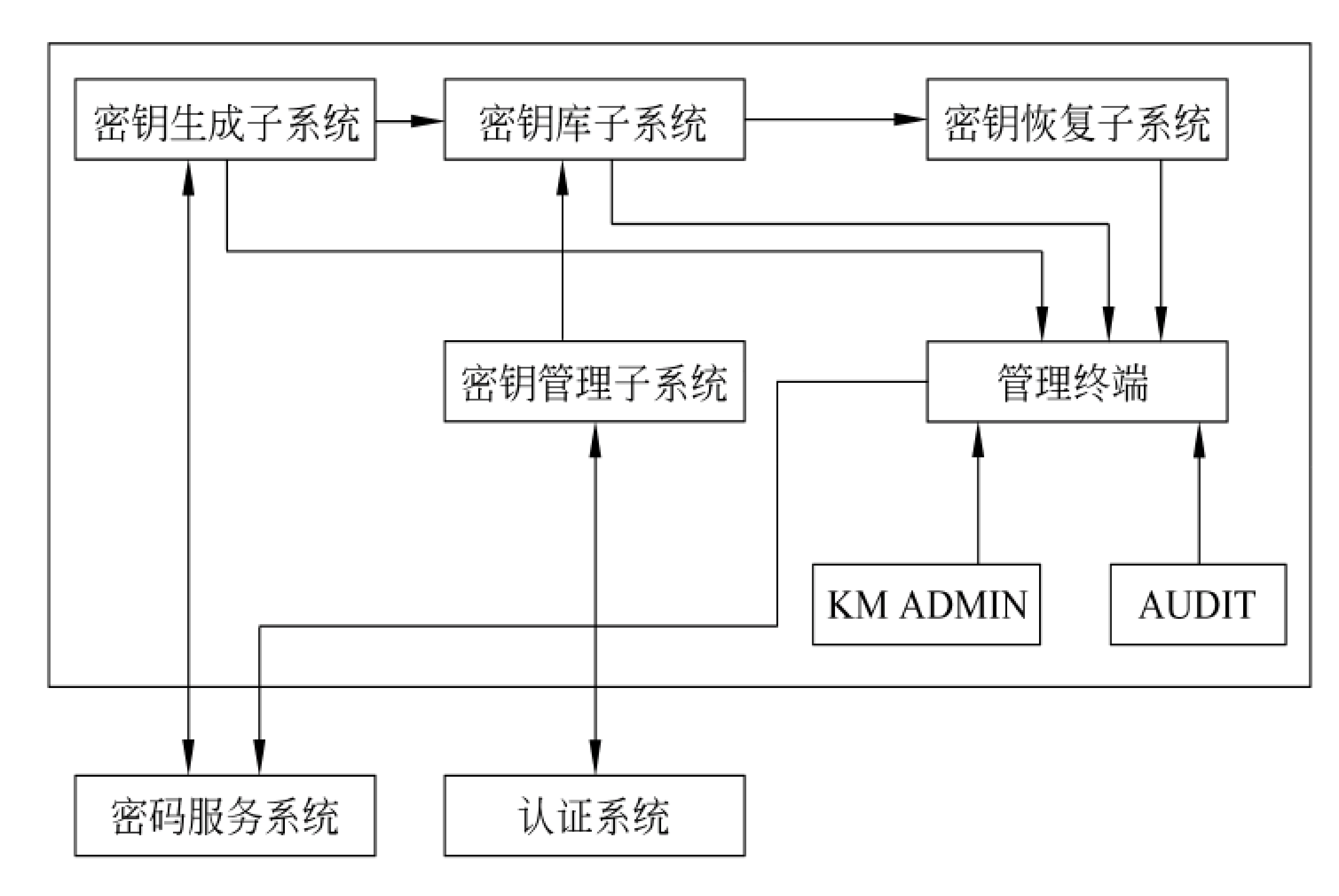


图 3-2-2 密钥管理系统逻辑结构图

事件无法访问原有加密数据的时候，密钥恢复子系统将用户原有密钥对进行恢复处理，以保证用户加密后的数据可以重新被访问。

(4) 密钥管理子系统：负责对整个密钥系统提供管理、配置。

(5) 管理终端：主要由 KM ADMIN 终端和 AUDIT 审计终端两个子模块组成。KM ADMIN 终端通过 C/S(客户机/服务器)结构的方式访问密钥管理服务器，提供对密钥管理系统具体的操作(包括启动密钥管理服务、配置密钥管理策略等)；AUDIT 审计终端提供记录、跟踪密钥管理服务的各项操作记录和相关的系统操作。

在具体的技术实现上，可以采用如图 3-2-3 所示的体系结构。

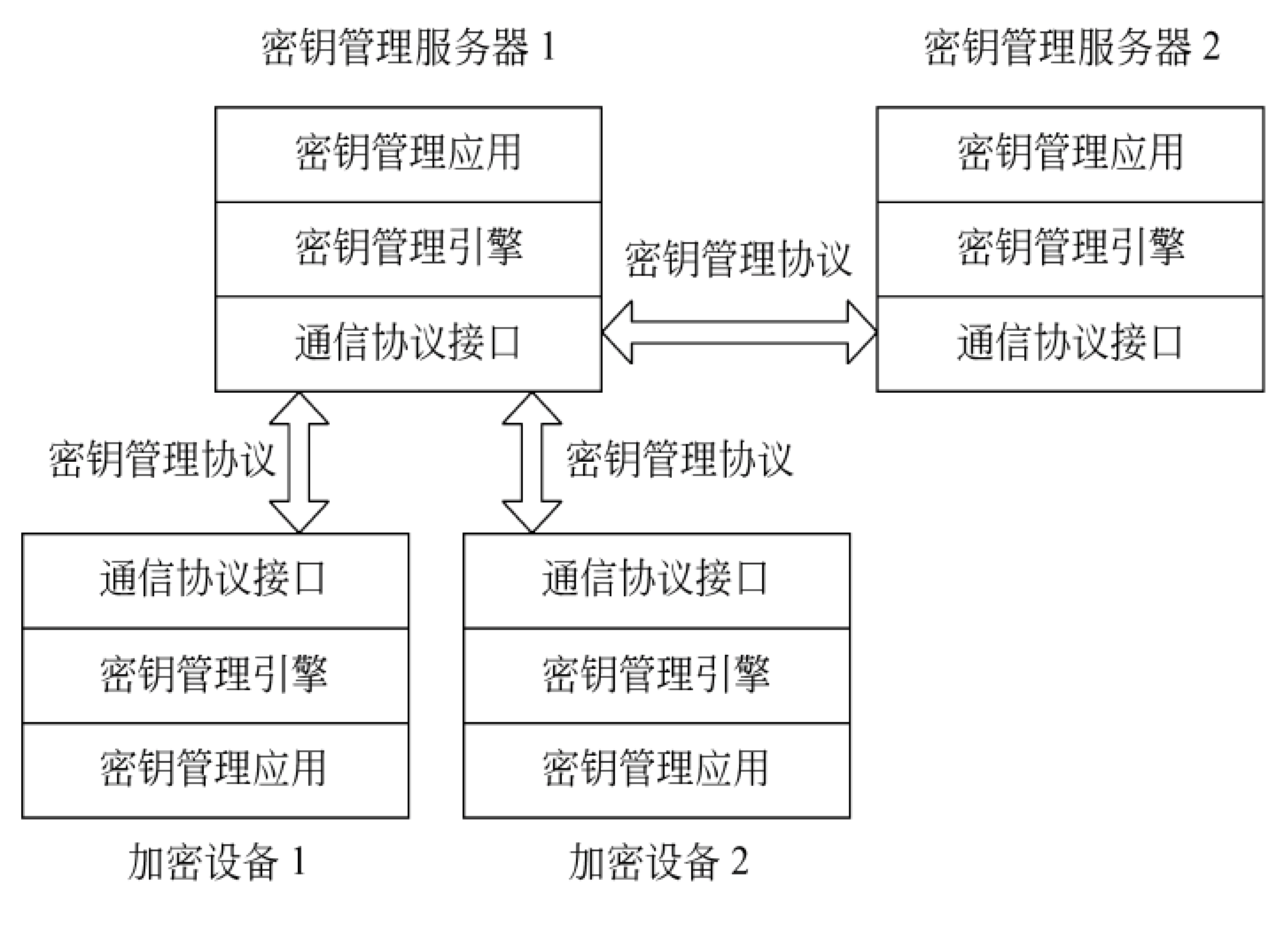


图 3-2-3 KMI 体系结构

技术实现上的标准化必须符合用户的使用要求，具体包括：总体结构采用分层按域管理的方式，核心操作区与对外服务区相隔离；用户界面稳定；管理信息库结构(SMI)设计具有检索方便、易于扩充的管理信息库结构；对所有管理对象属性进行抽象并进行形式化描述，使管理信息库(MIB)的设计具有普遍适应性；参照 SNMP 协议并结合密钥管理的特点，设计标准的密钥管理协议；基于加密设备标识、密钥标识设计安全协议。

3.3　认证技术

3.3.1　作用

当前最流行的认证技术是 PKI 技术。在某些情况下，也可以依据具体应用环境的安全需求，采用口令认证或基于生物特征识别的认证技术。实际应用中，上述几种认证技术往往结合起来使用，也称多因子认证技术。

一般地，认证体系由数字证书认证机构(CA)、数字证书审核注册中心(RA)、密钥管理中心(KMC)、目录服务系统、可信时间戳系统组成。由于这种认证体系以 CA 为核心，通常又称电子证书认证系统。该体系的作用主要是证书查询验证服务。

CA 是认证体系的核心，提供的服务主要包括：发放和管理证书；证书认证服务；管理证书撤销列表；设立、审核和管理注册中心。它负责对证书的整个生命周期进行管理。利用 CA 所签发的证书能够实现身份鉴别、实体认证、数字签名、数据加密和密钥协商等安全功能。

RA 是 CA 的延伸，是用户注册审核机构。注册中心由认证中心授权运作，提供的服务主要包括：证书申请的注册受理，审核用户真实身份，下载证书，设立、审核和管理证书受理核发点。

密钥管理中心是电子证书认证系统的一个重要组成部分，主要负责向 CA 提供密钥管理服务。密钥管理中心按照国家有关密码管理政策和法规为证书管理提供加密密钥的产生、登记、认证、分发、查询、注销、归档及恢复等管理服务，按照与认证中心统一规划、同步建设、有机结合、独立设置、分别管理的原则建设和管理。

目录服务是一种专门的数据库，是软件、硬件、策略以及管理的合成体，服务于各种应用程序。目录服务至少应包括以下几方面内容：

(1) 包含在目录中的信息。

(2) 保存信息的软件服务端。

(3) 扮演存取信息的软件客户端。

(4) 支持服务端,客户端软件的硬件。

(5) 支撑系统,如操作系统、设备驱动等。

(6) 连接客户端到服务端以及各个服务端之间的网络基础设施。

(7) 策略,规定谁能访问,谁能更新,谁能存取等。

(8) 维护和监视目录服务的软件。

认证体系中的目录服务涉及轻量级目录访问协议(Lightweight Directory Access Protocol,LDAP)和基于 X.500 的目录。这些目录都是通用的、标准的目录,不适合特定的操作系统和应用。其中,LDAP 轻量级目录访问协议,对 X.500 目录访问协议进行了简化,并且在功能、数据表示、编码和传输等方面都进行了相应的修改。目前,LDAP v3 已经在 PKI 体系中被广泛应用于证书信息发布、CRL 信息发布、CA 策略以及与信息发布相关的各个方面。

可信时间戳服务基于国家权威时间源和公开密钥基础设施 PKI 技术,为实际应用提供精确可信的时间戳,以保证系统处理的数据在某一时间(之前)的存在性及相关操作的相对时间顺序,为应用服务的不可否认性和可审计性提供支持。可信时间戳服务系统必须从国家权威的时间源获得全系统统一的时间,即从国家授时中心获取权威的时间。

证书查询验证服务系统为应用系统提供证书认证服务,包括目录查询服务和证书在线状态查询服务。证书查询验证服务系统主要包括 LDAP 服务器和 OCSP 服务器,提供包括各类证书发布、CRL 发布和证书状态在线查询服务。

3.3.2 基本模型

对于上述认证体系,通常认为它有三种基本的信任模型,分别是树状模型、信任链模型和网状模型。

1. 树状模型

在树状模型中,各结点按照一定的层次关系(即上下级关系)组织在一起,任意两个结点之间都可以通过它们共同的上级结点或者根结点(在整个树状模型中是唯一的)建立一条信任路径。这种模型对于层次结构关系明确的应用非常实用。例如,采用层次结构的机构(例如同一行业的中央级、省部级和地市级机构)所需的电子政务应用。

1) 树状模型的优点

(1) 具有树状模型的 PKI 证书便于许多应用的处理。

(2) 证书处理过程简单。

(3) 只需要安全地传递一个根证书就可以对子 CA 签发的证书进行认证。

(4) 撤销子 CA 的操作方便。

(5) 可以在一个规模很大的组织中通过组织证书策略，简单并且快速地撤销某个具有不同策略的子 CA 签发的所有证书。

(6) 信任传递关系简单。

(7) 可以用少量的 CA 证书管理大量的用户证书。

(8) 基于树状模型的 PKI 的应用能够与基于信任链模型 PKI 的应用之间进行互操作。

2) 树状模型的缺点

(1) 必须仔细保护根 CA 的密钥，因为根 CA 的密钥一旦丢失(或被破坏)将使整个系统的所有用户受到威胁(这些用户必须全部加载新的根 CA 证书)。

(2) 树状结构可能与某些机构的实际结构情况不符。

(3) 基于树状结构 PKI 的机构可能不具有交叉认证能力，不能与基于网状 PKI 的应用进行互操作。

2 信任链模型

在信任链模型中，各结点彼此间具有某种单一的信任关系，但并不具备层次关系。这种模型适用于形式松散，但又彼此间存在信任关系的机构，例如商业联盟、政府机构与企业的合作，以及某些情况下的电子政务外网。

1) 信任链模型的优点

(1) 广泛应用于商业环境中。

(2) 证书处理应用软件相对简单。

(3) 可以由每一个使用公钥的应用自行确定是否信任某个 CA。

(4) 不需要集中管理。

(5) 灵活性好。

(6) 与基于树状模型的 PKI 保持兼容，支持相互间的互操作。

(7) 信任关系错误传递的可能性较小。

2) 信任链模型的缺点

(1) 对信任关系的管理依赖于本地的网络管理员(可能不理解 PKI 或者不具备判断是否应该信任某个 CA 的能力)。

(2) 许多应用软件中预装有多种 CA 证书，用户虽然并不清楚这些 CA 所签发的证书的安全级别，却通常都信任这些证书。

(3) 缺少一种简单的证书撤销机制。

(4) 基于此类模型开发的 PKI 组件可能无法处理交叉认证，无法支持有关的互操作。

3. 网状模型

在网状模型中,各结点相互之间存在的信任关系比较复杂,不是严格的层次关系,也不是单一的信任链关系,而是呈现为错综复杂的网状关系。在电子政务的认证体系建设中,这种信任模型通常被用于不同行业的多个机构之间。

1) 网状模型的优点

(1) CA的信任关系符合现实的信任关系(例如,商业中的信任关系或其他非层次的信任关系)。

(2) 个人用户和网络管理员不用维护信任链表。

(3) 不受分布式管理信任链中的安全隐患的影响。

(4) 某个CA证书失效仅影响该CA的直接用户,不存在影响整个认证系统的根CA。

(5) 如果存在与基于树状模型的CA之间的交叉认证,在网状模型基础上开发的应用一般可以对基于树状模型的CA的证书进行验证。

2) 网状模型的缺点

(1) 在规模庞大的网状PKI中建立、验证信任链需要复杂的软件,并可能会影响处理的效率。

(2) 任一个CA都可以信任其他的CA,受信任的CA也可以信任组织之外的其他任何CA,网络结构的管理和证书的安全扩展必须仔细使用,以防证书链反映了错误的信任关系。

(3) 基于树状模型或信任链模型的PKI应用不能直接和基于网状模型的PKI进行互操作。

3.3.3 交叉认证与桥CA

认证体系中的一个关键问题是如何实现互操作。互操作问题和信任模型有关。例如,基于信任链模型开发的PKI组件可能不支持有关的互操作,而基于树状模型或信任链模型的PKI应用也不支持与基于网状模型的PKI应用之间的互操作。

解决互操作问题的途径有两种:交叉认证和桥CA。

交叉认证用于原先相互独立的不同认证体系的两个结点CA之间,目的是在这些认证体系之间建立信任关系,实现方法是由这两个结点CA向对方的根CA签发证书,从而支持这两个认证体系之间的互操作,如图3-3-1所示。

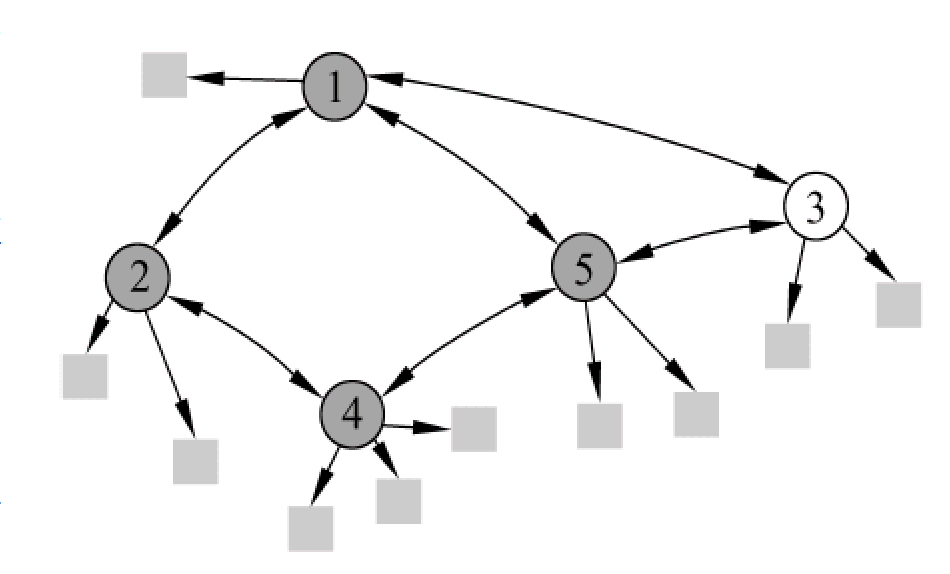


图3-3-1 交叉认证网信任模型结构图

在上述的网状模型中，任意两个结点间都采用双向交叉认证。

在交叉认证网模型中，如果没有命名空间的限制，那么任何 CA 都可对其他 CA 发证，所以这种结构非常适合表示动态变化的组织结构，但是在构建有效地认证路径时，很难在网中确定一个 CA 是否是另一个 CA 的适当的证书颁发者。很长的、跨越很多结点的、非层状的信任路径会被认为是不可信的，显然在这个模型中路径的构建比层次模型复杂得多，需要对不同 CA 发布的证书进行反复的比较，不但要建立一个从被验证方开始到验证者所在域的完整的信任路径，每一个验证者还需要建立自己到信任链的路径。其中的封闭环路一定要检测出来并丢弃掉，对可能存在的多路径要用策略进行过滤和优先级的设置。

桥 CA 是交叉认证的一个特例，它与原先彼此独立的各个信任体系的根结点进行交叉认证，从而在这些根结点之间建立信任关系，如图 3-3-2 所示。

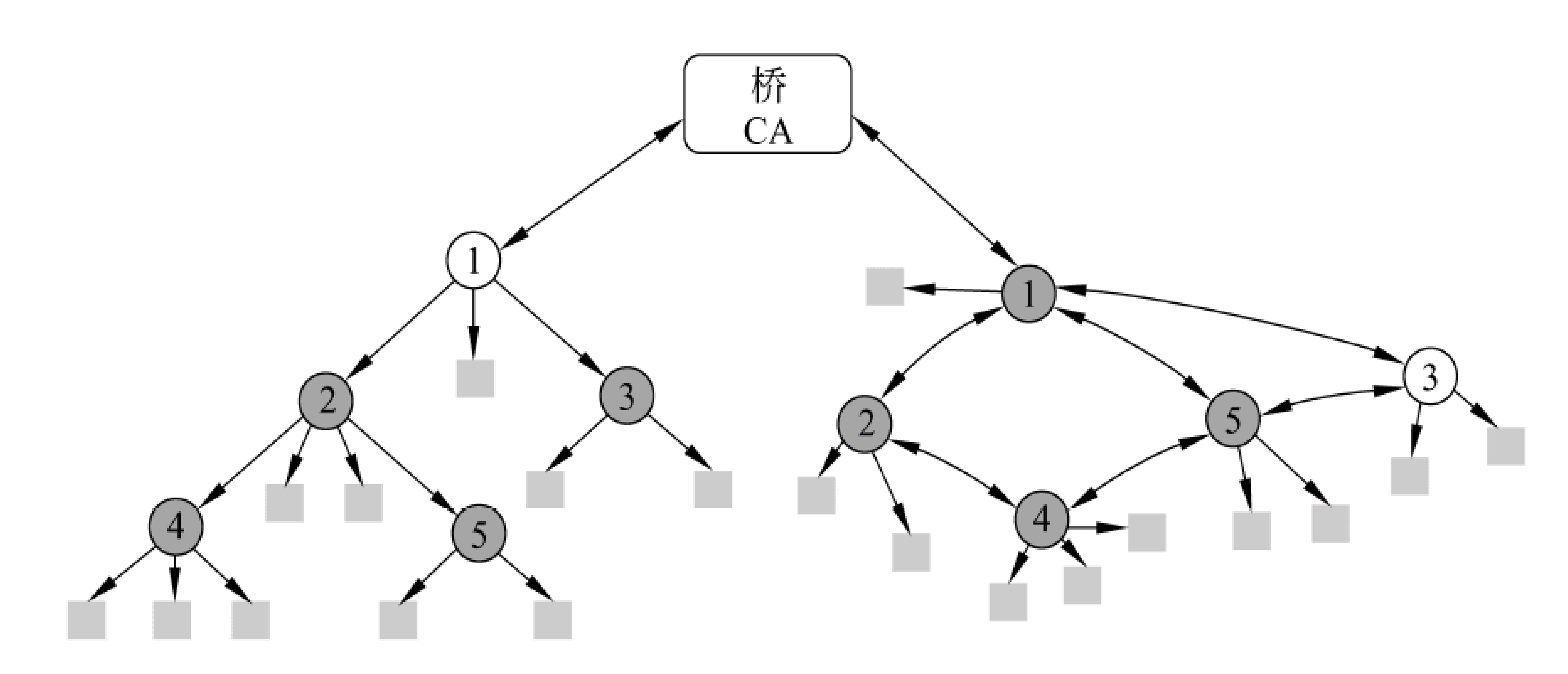


图 3-3-2　桥 CA 信任模型结构图

对于小规模的 PKI 应用，可以在树状模型基础上采用交叉认证。但是如果 PKI 应用规模较大，根与根之间的交叉认证就会变得相当庞大，交叉认证不便于解决这种问题，所以产生了桥式结构，又称桥 CA 模型。这种结构被美国联邦 PKI 所采用。

桥 CA 模型实现了一个集中的交叉认证中心，它的目的是提供交叉证书，而不是作为证书路径的根。对于各个异构模式的"根"结点来说，它是它们的同级，而不是上级。当一个企业与桥 CA 建立了交叉证书，那么，他就获得了与那些已经和桥 CA 交叉认证的企业进行信任路径构建的能力。

显然，桥 CA 模型中在域间也可确定一条唯一的信任路径，桥 CA 是在大量组织中扩展 PKI 的一种重要方法。但是桥 CA 必须要有一个大家都信任的第三方来充当桥 CA，它要和所有的域进行交叉认证，并且管理所有的策略映射，在实践中是很难确立这样一个第三方的。

3.3.4 体系结构

1. CA结构

如图 3-3-3 所示，一个完整的 CA 系统从逻辑上来说，主要包括以下四部分。

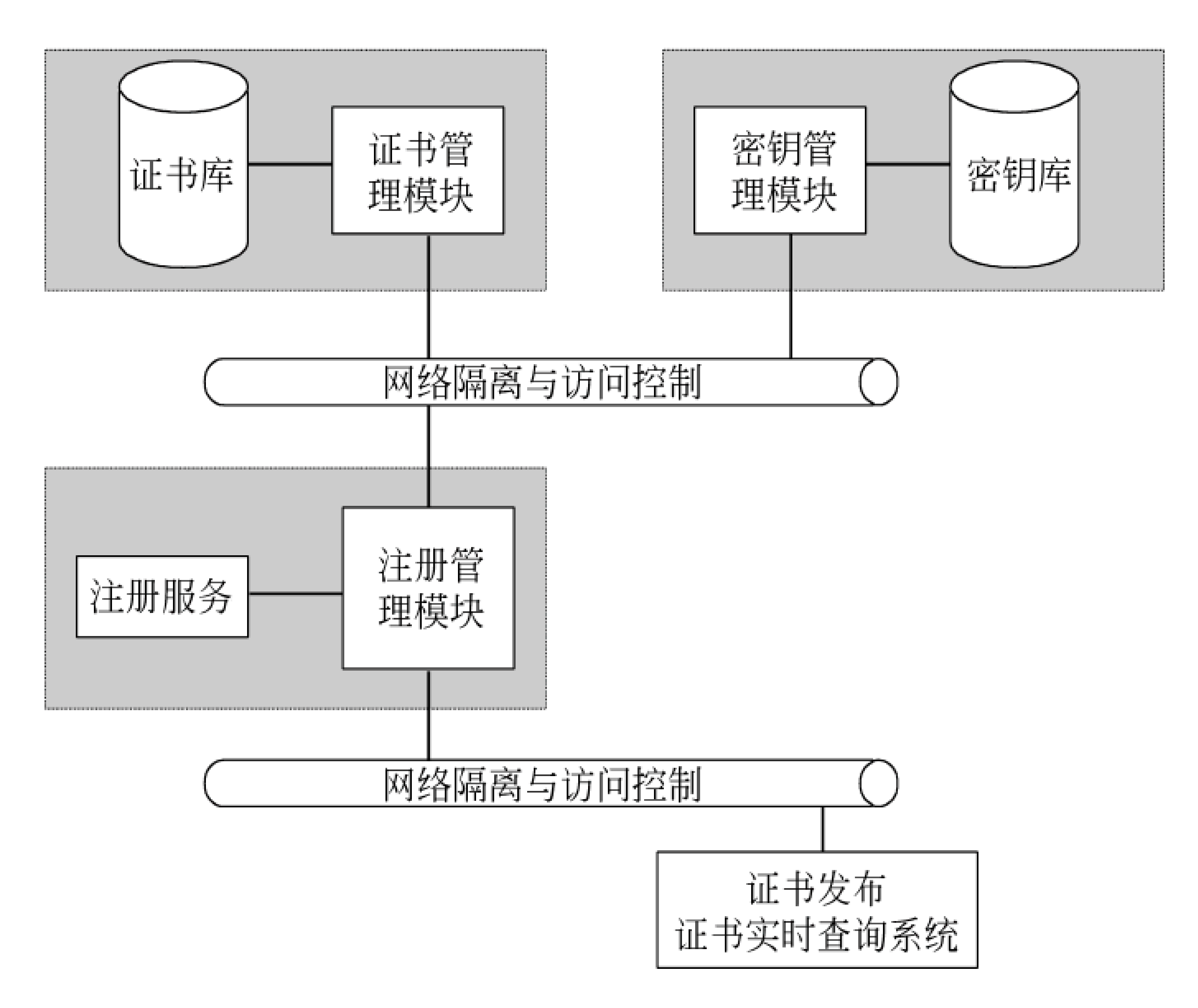


图 3-3-3　CA 系统的逻辑结构

1）证书管理模块

CA 系统的核心模块，用于生成/签发并管理公钥证书和证书撤销列表，负责证书库的维护。

2）密钥管理模块

用于生成、管理 CA 系统所需的密钥，管理、维护密钥库。

3）注册管理模块

CA 系统面向最终实体(用户、服务器等)的接口，负责接受证书申请，管理最终实体申请信息，审核和执行对最终实体的相关操作。

4）证书发布及实时查询系统

可集中存储所有最终实体的证书信息，并向全系统发布可以公开的证书信息和证书撤销信息，提供证书状态在线查询服务。

上述四部分根据重要程度不同分别采用网络隔离或其他访问控制措施将其划分开来。

其中，CA 的结构设计通常遵循两种思路：集中式和分层式。集中式 CA 通过一个统

一的 CA 中心进行集中管理和负责统一维护，结构简单，但是工程实施难度较大。分层式 CA 采用分层设计（例如，在电子政务应用中，按照行政级别分为部级、厅级和局级这三层）进行分散管理和统一协调，结构比较复杂，但是工程实施比较容易，并且和电子政务中许多机构自身的层次化组织形式相符。

CA 的具体结构设计需要结合实际应用需求的特点。一般认为，这主要取决于应用机构的规模大小和业务量的大小。对于规模和业务量小的机构，集中式的 CA 简单易行，成本也较低。对于规模和业务量大的机构，尤其是对于自身具有层次化组织特点的机构，建立统一的 CA 中心管理和维护困难并且成本较高，采用分层式 CA 则能够明显降低工程实施的复杂程度，同时也能够调动下级机构参与管理的积极性。

在具体的 CA 应用中，证书管理通常包括：证书申请，证书签发，证书的存储与发放，证书查询，证书撤销和证书删除。证书申请有两种方式，即在线申请方式和离线申请方式。证书签发可以依据用户需要签发单证书或双证书。前者指签名证书，后者指签名证书和加密证书。

2 RA 结构

RA 结构主要有两种，即独立式 RA 和嵌入式 RA。

独立式 RA 的体系结构如图 3-3-4 所示。

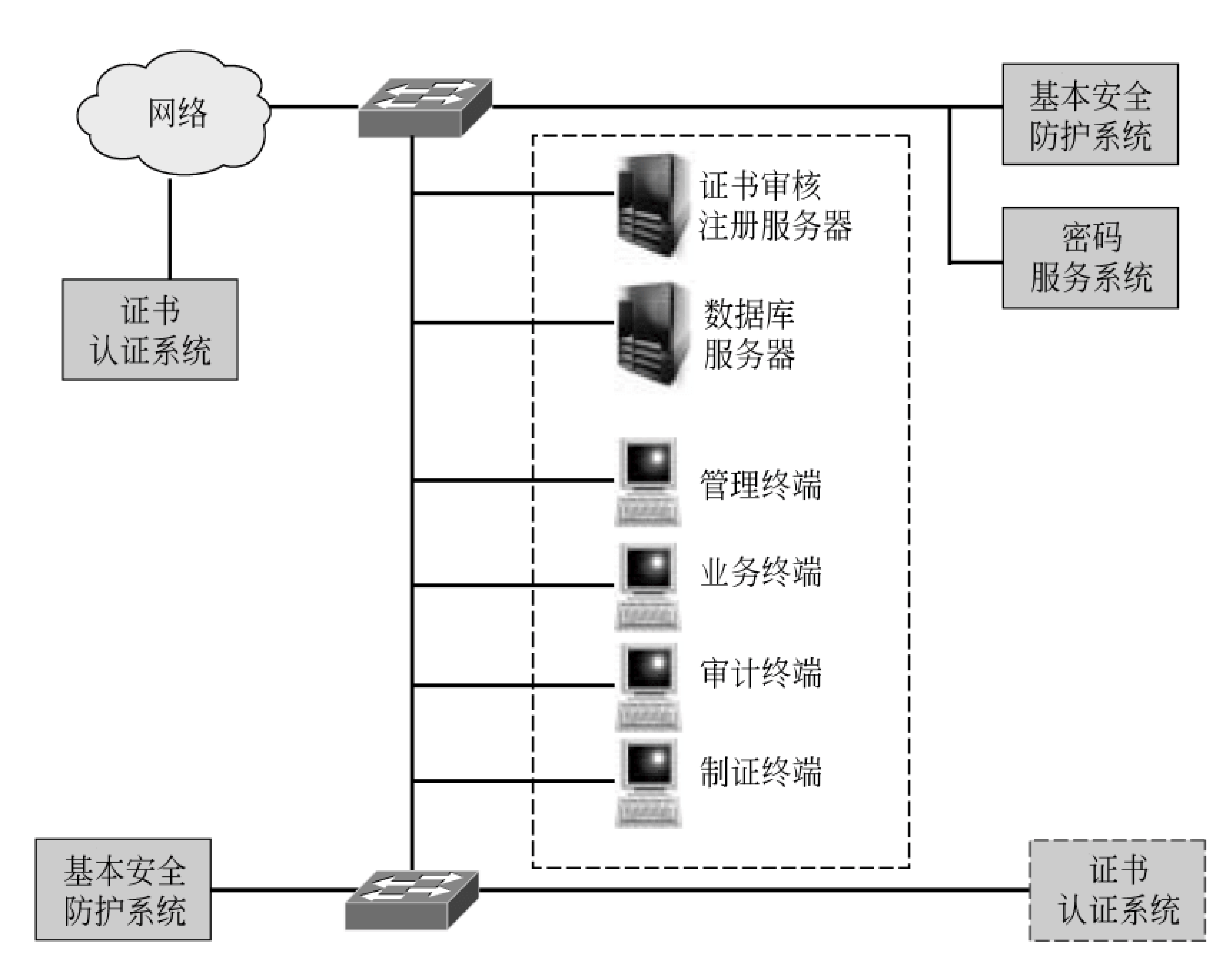


图 3-3-4　独立式 RA 体系结构图

在独立式 RA 体系结构中，RA 中心由证书审核注册服务器、数据库服务器、各类终端、基本安全防护系统和密码服务系统组成。如果是本地 RA，则 RA 与后面交换机相连的证书认证系统进行交互，如果是远程 RA，则 RA 与网络上的证书认证系统进行相连。

RA 采用客户端/服务器结构，包括 RA 服务器、RA 客户端。RA 客户端由录入、审核、管理、审计四个模块组成，完成证书申请和管理的工作，如图 3-3-5 所示。

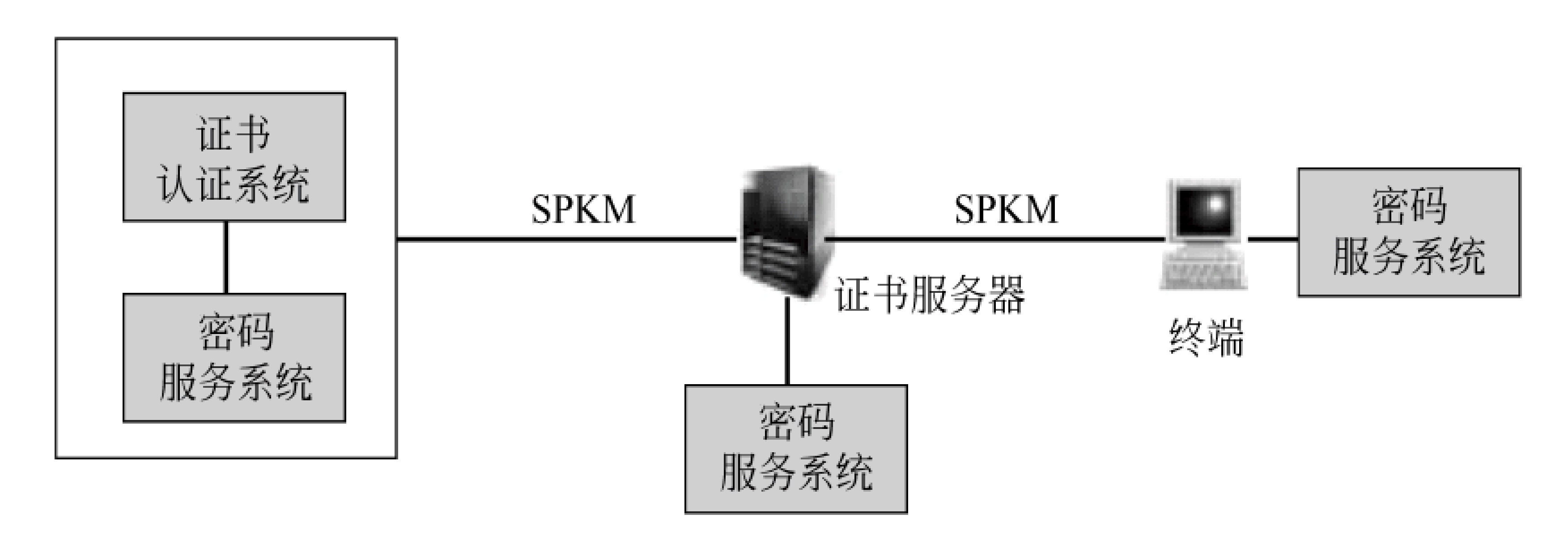


图 3-3-5　RA 体系结构

RA 客户端通过 RA 服务器进行数据通信，每个 RA 客户端与 RA 服务器之间以及 RA 服务器与证书认证系统之间都采用 SPKM 协议进行加密通信，以保证系统通信的安全性。

嵌入式 RA 的体系结构是根据机构的业务特点并通过采用 RA 前置机系统，其系统结构如图 3-3-6 所示。其工作原理是：首先，通过在机构原有的业务系统中嵌入证书注册服务代理模块，接收用户证书管理请求；接着，证书管理请求通过这些业务系统将数据传

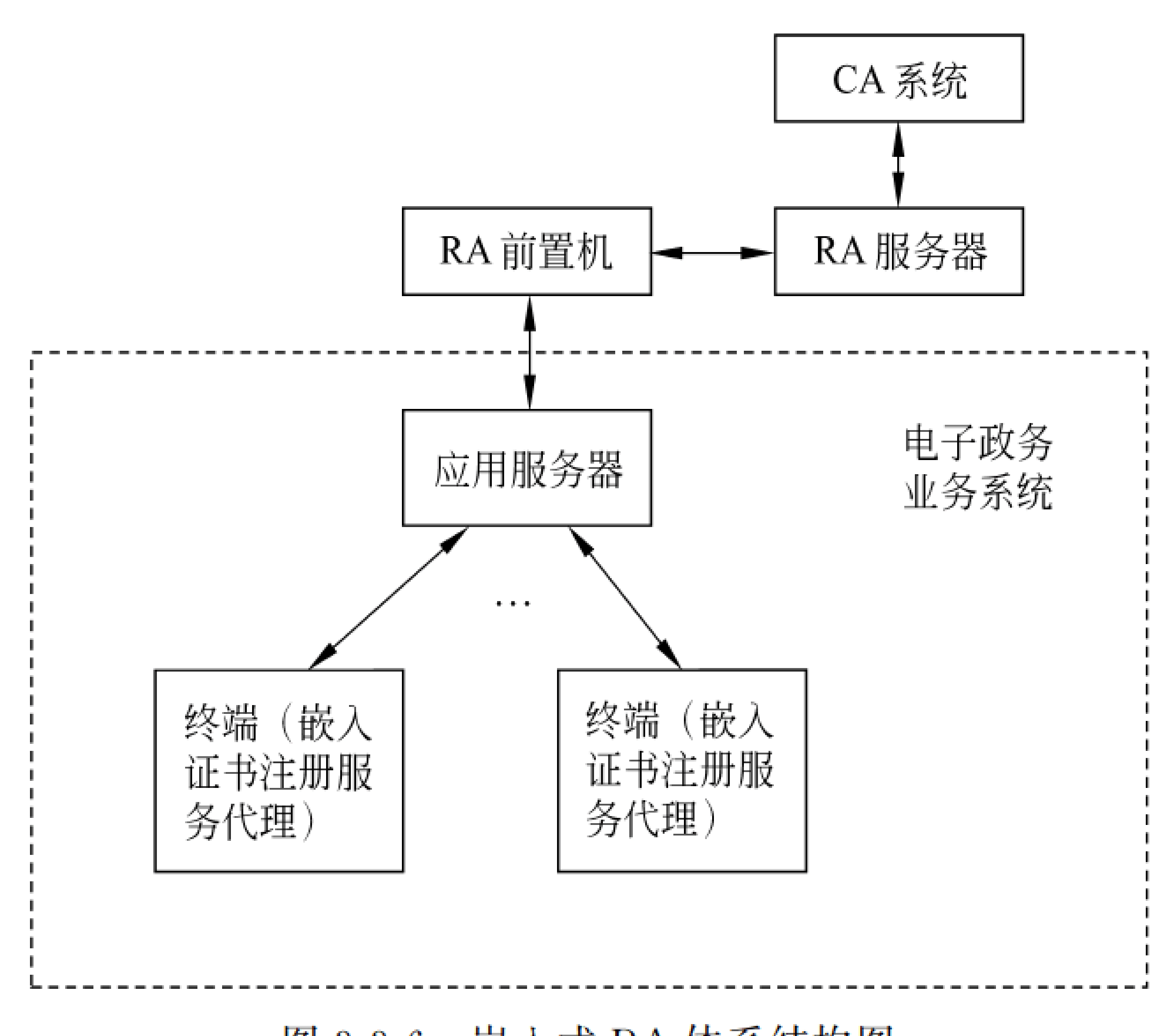


图 3-3-6　嵌入式 RA 体系结构图

入 RA 前置机；最后，RA 前置机通过安全的模式将数据格式转换为认证系统能够识别的数据，从而完成数据的上传和下载过程。

嵌入式 RA 体系结构的特点是：减少投资、节省人力；容易实现数据共享；便于管理；具有良好的灵活性；系统更加友好，使用者不需要另行培训。

3. 可信目录服务的结构

设计可信目录服务的核心是目录树的结构设计。目录树提供了一种对目录数据进行组织的方法（例如按照部门、地理位置、工作性质等方式组织用户数据）。目录树的结构设计为目录数据的命名和应用访问提供基本框架。这种设计应符合 LDAP 层次模型，并且遵循以下三个基本原则：

（1）有利于简化目录数据的管理。

（2）可以灵活的创建数据复制和访问策略。

（3）支持应用系统对目录数据的访问要求。

公钥证书系统的目录服务结构设计如图 3-3-7 所示。

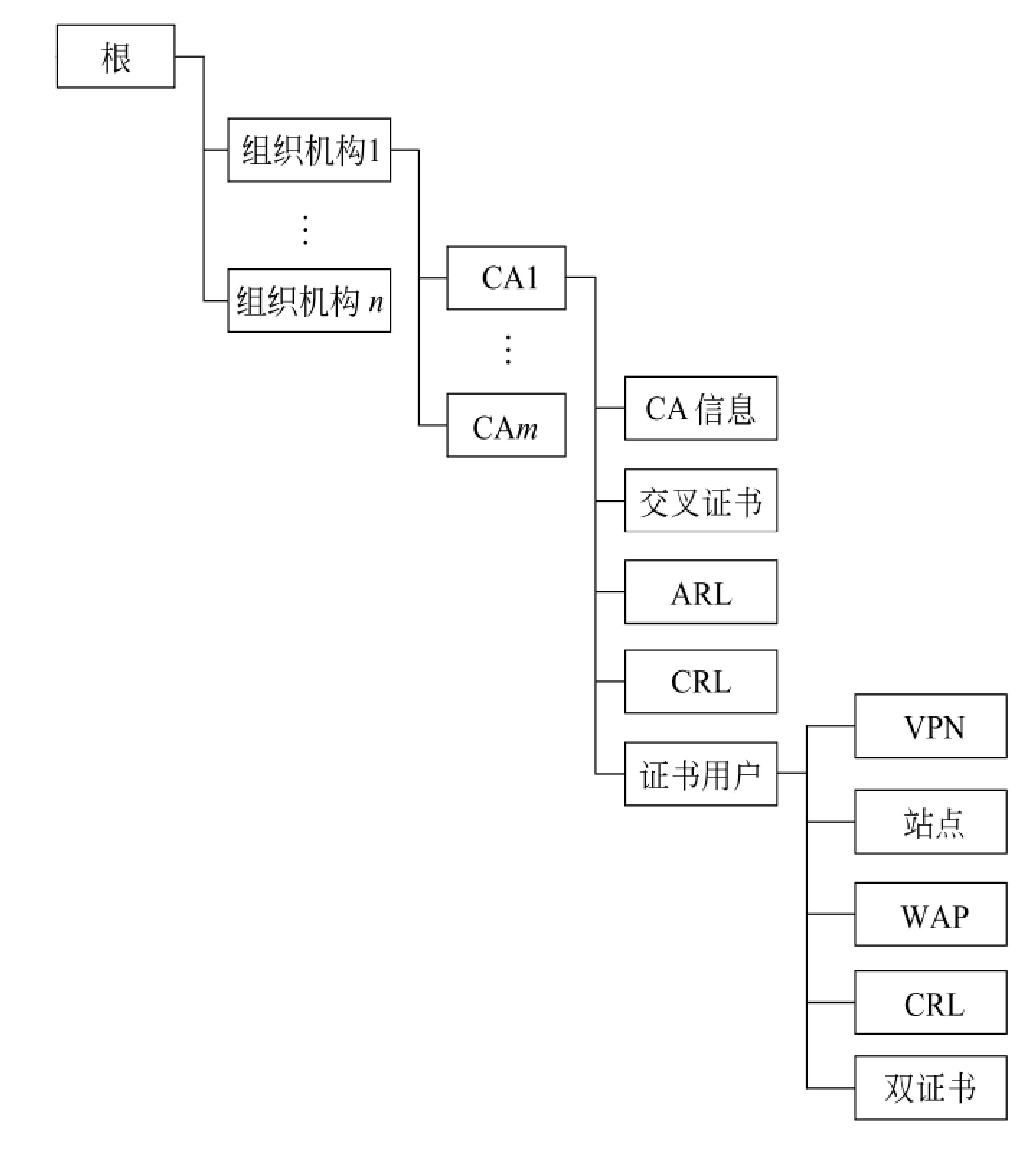


图 3-3-7　公钥证书系统的目录服务结构设计

4. 可信时间戳的体系结构

可信时间戳服务系统的体系结构如图 3-3-8 所示。其中,各主要组成元素的作用分别是:

(1) 时间服务器:通过国家授时中心为时间戳服务提供可信时间服务,监控并校准时间戳服务器的时间。

(2) 时间戳证据存储服务器:安全存储时间戳及其相关数据。

(3) 时间戳服务器:为请求数据签发可信的时间戳。

(4) 密码服务系统:为时间戳服务提供基本的密码操作。

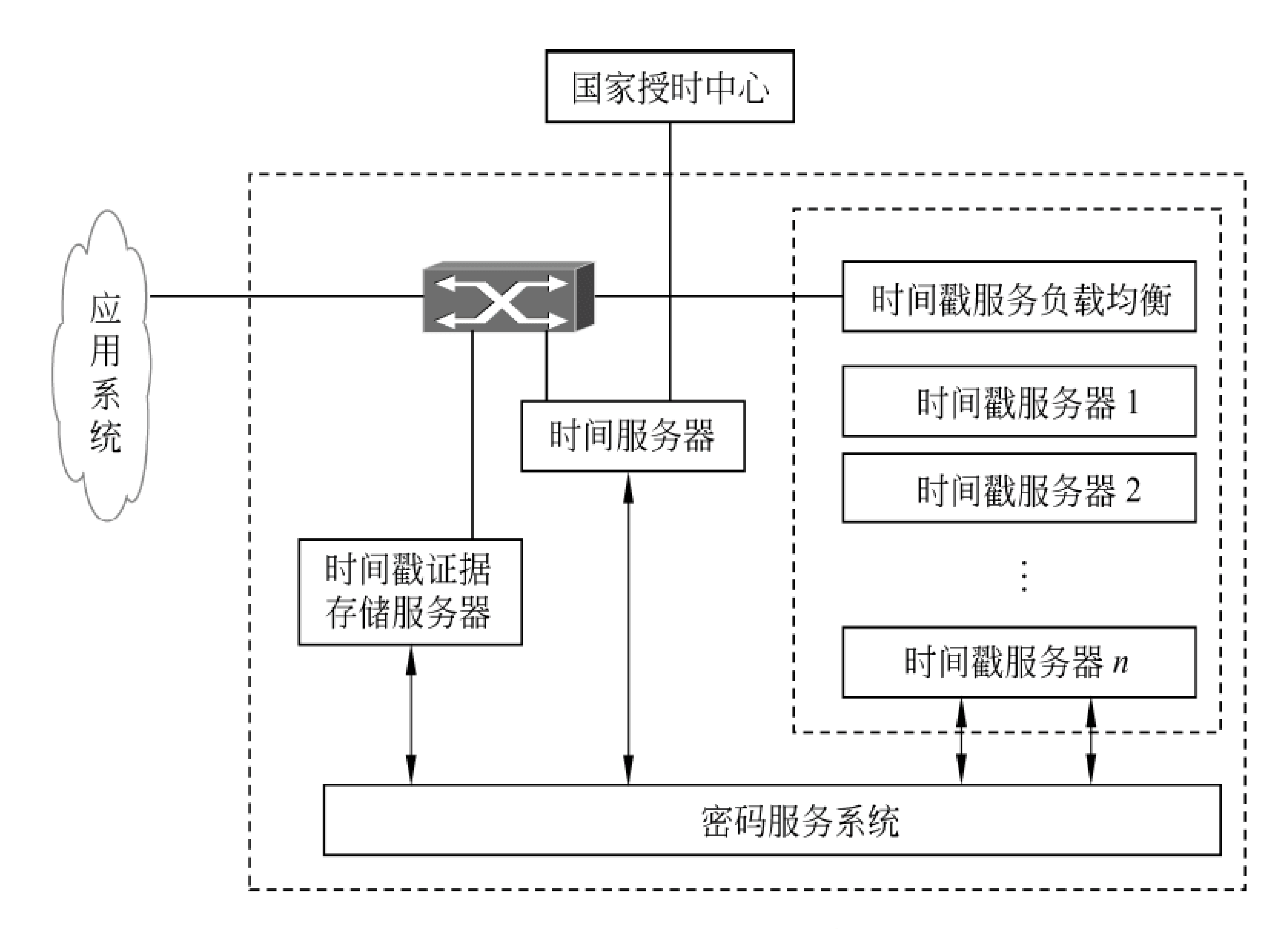


图 3-3-8 可信时间戳服务系统体系结构

5. 证书查询验证服务系统的应用模式

证书查询验证服务系统的应用模式如图 3-3-9 所示。

当客户端访问服务端应用时,需要向服务器证明其合法身份。此时,客户端会提交能够证明用户身份的身份证书,证书查询验证服务就会验证用户证书的颁发机构是否可信、证书的签名是否有效、证书是否过期。当这些验证都通过后,证书查询验证服务系统就会去 LDAP 服务器或者 OCSP 服务器请求验证用户证书是否已经被吊销。LDAP 里存储了 CRL(证书黑名单列表),所有被系统吊销的用户证书信息都被登记在 CRL 中,而 OCSP 则需要有应用程序调用 OCSP API 访问 OCSP 服务器,查询用户证书此时的状态。OCSP 会返回"有效、无效、未知"三种状态,应用服务器根据返回结果来验证用户的真实身份。

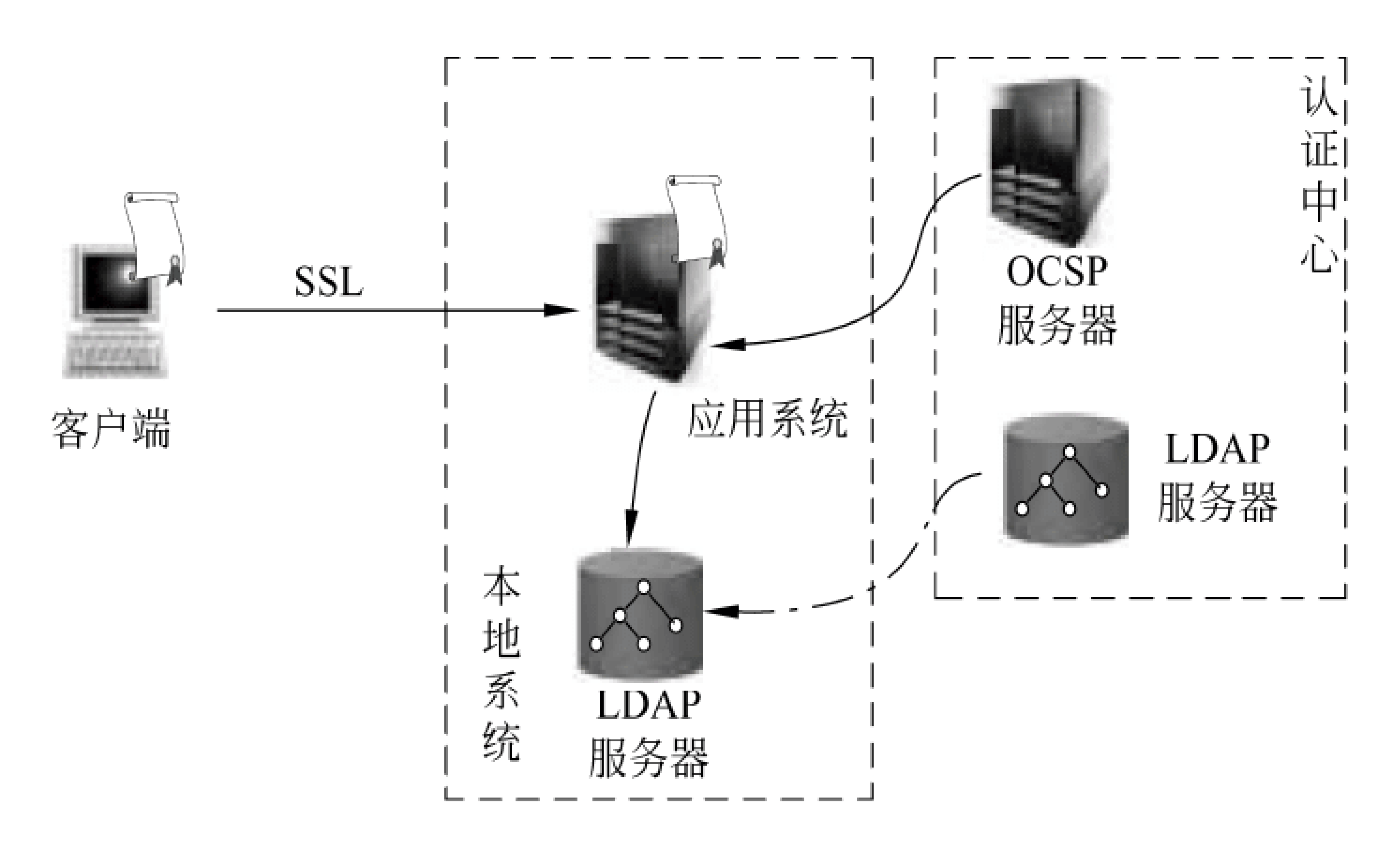


图 3-3-9　证书查询验证服务系统的应用模式

3.3.5　主要组件的功能要求

主要包括 CA、RA、密钥管理中心 KMC、可信目录服务、可信时间戳的功能要求。

1. CA 的功能要求

下面介绍 CA 的功能要求。

1）Web 方式的服务

提供数字证书认证中心的安全可信的 Web 方式的服务。

2）证书/证书撤销列表签发服务

（1）支持 X.509 v3 或 X.509 v4 证书格式。

（2）支持 X.509 v2 证书撤销列表格式。

（3）采用国家密码主管部门审批的签名算法完成签名操作，提供各种数字证书及证书撤销列表的签发服务。

3）证书管理服务

主要是对各种数字证书、内部管理员证书及操作员证书进行管理。

4）证书撤销列表管理服务

（1）提供证书撤销列表的操作策略及管理策略。

（2）安全管理证书撤销列表。

（3）证书撤销列表的生成。

（4）证书撤销列表的更新。

（5）证书撤销列表的发布。

5）密码服务

（1）采用国家密码主管部门审批认可的加密及签名算法。

（2）建立密码服务机制。

（3）采用国家密码主管部门审批的密码设备提供密码服务，实现安全的证书签发等功能。

（4）私钥必须存储在硬件密码设备中，硬件密码设备须具备密钥备份管理机制，并应具备设备安全和敏感信息保护机制；设备的真实性鉴别；私钥导入应采取安全处理措施。

（5）对内部软件模块提供统一调度管理。

（6）支持密码设备动态按需加载并且不中断系统密码服务。

（7）提供系统的可信日志审计及统计服务。

（8）提供系统运行状态管理，对设备运行进行监测和控制。

6）数据管理服务

（1）提供数据安全管理与维护。

（2）管理机构、设备、内部人员的证书申请信息、证书信息、证据、认证策略信息、操作策略信息、业务操作日志等。

（3）核心数据的加密存储。

（4）数据备份功能。

（5）数据库的防攻击、防灾害功能。

7）目录管理服务

（1）基于 LDAP 技术的目录访问控制服务。

（2）证书库和证书撤销列表的发布。

（3）证书库和证书撤销列表的下载。

（4）证书库和证书撤销列表的更新。

（5）证书库和证书撤销列表的恢复。

（6）证书库和证书撤销列表的实时状态查询功能。

（7）基于 OCSP 技术的证书状态在线查询服务。

8）交叉认证服务

需要时，提供各种电子业务的数字证书，认证中心提供交叉认证服务。

9）日志服务

（1）记录管理员和操作员的所有动作。

（2）记录整个证书认证系统中各子系统的内部运行错误和异常。

（3）对整个 CA 体系的发卡数量做实时统计和分析。

（4）提供查询、分析和审计管理。

(5) 提供统计报表输出。

(6) 对日志进行备份。

10) 动态扩展

(1) 证书认证中心的主要功能模块随着业务量的增加,可动态增加相应的模块单元,如 Web 服务单元、应用服务单元等,以适应业务扩展的需求。

(2) CA 系统的体系结构能够依据需要进行纵向扩展。

11) 用户服务

(1) 个人证书管理：通过界面友好、操作简单的个人证书管理的客户端软件帮助用户管理和维护自己的数字证书,提供个人证书定制服务。

(2) 证书到期更新通知服务：基于 C/S 或 B/S 模式对证书进行统计查询,制定更新规则并自动发送提示信息。

(3) 用户证书统计报表服务：为提高对于用户服务请求的响应速度,自动搜集关于证书的请求、状态等信息,并进行必要的分析和统计,形成可视报表。

12) 用户服务功能的扩展

可根据业务需求以及用户个性化需求,通过简便易行的方式添加新的服务功能模块。

2 RA的功能要求

RA 的功能要求如下。

1) Web 服务

提供安全可信的 Web 服务,具体包括：数据流加解密、信息完整性验证、身份鉴别、信息抗否认和访问控制。

2) 用户服务功能

(1) 证书注册：完成用户信息注册功能。

(2) 用户审核：根据 RA 操作规程和制定的审核策略审核用户的注册信息是否正确无误,自动向用户反馈有关消息。记录每次审核日志,提供工作量统计,处理跟踪分析,处理异常情况分析。

(3) 证书申请：受理用户的证书申请,将合法申请转发至 CA 中心,请求 CA 中心为合法用户签发证书。

(4) 证书下载：通过可信的 Web 服务,使用户可以在线下载所申请的证书。

(5) 证书注销：负责将用户申请注销证书的申请转发至 CA 中心,当得到用户确认后注销该证书。

(6) 证书更新：受理各种证书更新申请,负责将申请转发至 CA 中心。

(7) 密钥恢复：通过一定的审查验证策略,为用户向 CA 中心请求恢复加密密钥,提

供用户加密密钥恢复功能。

3）证书管理服务

（1）提供证书认证策略及操作策略的管理。

（2）对自身证书进行安全管理。

（3）对内部管理员数字证书、操作员数字证书进行统一管理。

（4）支持批处理方式发放证书。

4）密码服务

（1）用国家密码主管部门审批认可的加密及签名算法。

（2）用国家密码主管部门审批的密码设备提供密码服务，实现安全的证书签发等功能。

（3）密钥必须存储在硬件密码设备中，硬件密码设备须具备密钥备份管理机制，并具备以下三项具体功能：应具备设备安全和敏感信息保护机制；设备的真实性鉴别；私钥导入过程必须安全。

（4）对内部软件模块提供统一调度管理。

（5）支持密码设备按照需要动态地加载，并且密码设备的加载不能中断系统密码服务。

（6）提供系统的可信日志审计及统计服务。

（7）提供系统运行状态管理，对设备运行进行监测和控制。

5）数据管理服务

（1）提供数据安全管理与维护。

（2）管理机构、设备、内部人员的证书申请信息、用户资料、证书信息、证据、认证策略信息、操作策略信息、业务操作日志等。

（3）核心数据的加密存储。

（4）数据备份。

（5）数据库的防攻击与防灾害。

3. 密钥管理中心的功能要求

密钥管理中心（KMC）的功能要求如下：

（1）密钥管理策略的制定。

（2）密钥生成与存储：在双密钥证书系统中，用户密钥中的加密密钥对在密钥管理中心生成，签名密钥对在用户端或者用户端授权的可信第三方生成。密钥管理中心为用户生成密钥对并负责保存，生成加密密钥对后由 CA 中心以安全的方式分发给用户。

（3）密钥分发：证书是密钥分发的一种有效方式，用户密钥生成后发送给认证中心，

由认证中心完成对包含密钥的证书的签发和管理。密钥管理中心也可以采用带密码运算的 IC 卡来安全管理用户密钥。

（4）密钥查询：当用户（主要是密钥的合法使用者，或者需要得到有关的密钥信息并进行执法工作的特殊用户）需要查询密钥信息时，需要向 CA 中心提交用户申请表，CA 中心在进行证书验证并许可后，将用户申请表及用户证书提交给密钥管理中心，密钥管理中心将对应的历史信息链从数据库中取出，并利用用户证书制作数字信封后，发送给 CA 中心，由 CA 中心交给用户。

（5）密钥恢复。

① 密钥恢复确保用户在忘记了存储密钥的口令，或者存储密钥的智能密码钥匙遭到破坏的情况下继续使用其密钥。

② 对于用户申请的密钥恢复服务，必须通过指定的管理人员进行相关操作，具体过程是：首先向 CA 认证中心提出密钥恢复申请，CA 认证中心收到用户的密钥恢复申请并核验该用户的合法身份后，将用户的密钥恢复请求转发给密钥管理服务器；密钥管理服务器在确认 CA 中心转发的密钥恢复请求为合法后，从其所托管的密钥库中恢复所需要的托管密钥记录，签名加密后，返还 CA 认证中心，CA 认证中心再将收到的密钥信息安全地返还用户；CA 认证中心返回给密钥管理服务器一个确认。

③ 在上述密钥恢复过程中，所有密钥恢复请求信息、返还密钥记录信息都必须经过签名和加密，以保证密钥记录和请求来源的完整性、机密性和不可否认性。

（6）密钥备份。

① 为确保重要数据不被丢失，必须对用于解密的私钥进行备份。

② 如果密钥对已经生成但尚未被用户使用，KMC 对其进行加密并将其存入预生成数据库。

③ 如果密钥对已经生成并被用户使用，KMC 对其进行加密并将其存入密钥数据库，以便在需要时进行恢复和查询操作。

（7）密钥归档。

① 在进行密钥更新时，为了保证以前加密的数据不丢失，需要对用于解密的私钥进行归档。存档的时间由安全策略决定。归档后的密钥形成历史信息链，供用户查询或恢复。

② 密钥更新时，密钥管理中心需将旧的密钥归档，即将正在使用数据库中该用户的密钥转入归档数据库，并插入对应的历史信息链中，供以后用户恢复及查询。

（8）密钥托管：在用户密钥丢失或需要调查取证等情况下，从系统提供的信息中获取用户密钥，解密用户加密的数据，以还原用户密钥或获取需要的证据。

（9）密钥销毁：密钥管理系统必须以安全的方式销毁过期的、丢失的和等待更新的

密钥。

(10) 密钥更新：在更新某个密钥之前，必须首先确认原密钥已经被安全销毁。

4. 可信目录服务系统的功能要求

可信目录服务系统的功能要求如下：

(1) 证书发布功能：LDAP 服务系统为证书业务服务系统提供证书发布、证书更新服务，为用户提供证书下载服务。

(2) CRL 发布功能：LDAP 服务系统为证书业务服务系统提供证书撤销列表(CRL)发布、证书撤销列表(CRL)更新服务，为用户提供 CRL 下载服务。

(3) 同步功能：LDAP 服务系统以分布式方式提供服务，目标 LDAP 通过和 CA 中心源 LDAP 系统同步来实现此功能。方便用户下载证书和 CRL 列表。

(4) 属性证书的发放功能：LDAP 服务系统为属性证书业务服务系统提供证书发布、证书更新服务，为用户提供证书下载服务。

(5) ACRL 列表的发布：LDAP 服务系统为属性证书业务服务系统提供证书撤销列表(ACRL)发布、证书撤销列表(ACRL)更新服务，为用户提供 ACRL 下载服务。

(6) 采用负载均衡技术，系统具备可伸缩配置及动态平滑的扩展能力。

(7) 可以根据业务量大小动态增减服务单元，调整系统业务能力。

(8) 可以有效地抵御各种常见攻击行为。

5. 可信时间戳的功能要求

可信时间戳的功能要求如下：

(1) 时间服务器通过时间接收设备从可信时间源获取时间，同时与时间戳服务器进行对时。

(2) 时间戳证据存储单元安全保存时间戳，确保数据的可审计性，实现系统数据处理的抗否认性。

(3) 时间戳服务负载均衡模块，实现分布式计算，确保时间戳服务的高效性、有效性和持续性。

(4) 时间戳服务器通过公钥基础设施(PKI)技术，为符合请求格式的数据加盖可信的时间戳。

(5) 时间服务器从国家授时中心获取权威的时间。

6. 证书查询验证服务系统的功能要求

证书查询验证服务系统的功能要求如下：

(1) 在线发布、查询和下载证书。

① CA 系统的证书查询功能主要采用 LDAP 协议。CA 系统可以对证书进行在线发

布。CA 系统签发证书后，将用户的证书发布到系统的主目录服务器中，然后利用目录服务器的自动映射功能，将用户的证书发布到从目录服务器中，以供用户在线查询证书。同时提供 Web 查询证书方式。

② 用户可以在查询证书信息后下载证书。系统支持在线的方式获取用户证书，同时支持在 CA 中心对外服务的目录服务器中查询其他用户的证书。

(2) 查询和下载 CRL。

① 采用 CRL 分布点技术存储 CRL。CRL 分布点采用分布式存储技术，解决了 CRL 增量问题。CRL 的增长不会给系统带来额外的负担。

② 系统中采用了 CRL 分布点技术，当用户选择下载 CRL 进行查询时，下载的信息并不是 CA 中心 CRL 的全部，只是其中的一个子集，这样就大大地减少了信息量，提高了查询的速度，降低了网络的负担。

③ CRL 的签发可分为"立即签发"与"定时签发"两种，用户可根据组织的安全策略进行选择和使用。

(3) 查询证书的在线状态。

① 由于 CA 注销表是周期性签发，并非是实时的，即使其周期特别短，在对证书状态实时性要求比较高的应用中，CRL 验证并不能够满足需求。

② CA 系统提供对证书在线状态查询协议的支持，用户可以通过标准的证书状态查询接口来获取证书有效性的检查结果。

③ 提供在线证书状态查询(OCSP)功能以满足实时证书验证的要求，任何证书的作废应能够即时反映到在线证书查询中。

(4) 验证证书的有效性。

(5) 验证证书签名信息。

(6) 验证证书链。

3.3.6　其他认证技术

除上述基于 PKI 的认证机制之外，实际应用中也经常依据具体应用环境采用口令(包括个人识别号 PIN)认证、生物特征识别等非密码的认证机制。

口令认证是最简单、使用最为普遍的认证机制。但是，它具有一些明显的脆弱性，包括：外部泄露、口令猜测、线路窃听、口令重放等。此外，它也可能对口令验证者带来安全隐患，导致口令验证者为非法用户提供服务。口令认证机制的安全性依赖于多种因素，最主要的是口令自身的强度、口令管理和口令系统的设计方法。

一般地，应该采用满足以下要求的强口令，这是针对口令猜测的最基本的防护方法：口令长度至少为 8 位；口令中应该包括数字、英文字母(包括大、小写)、特殊符号。

以下是基本的口令管理方法：

（1）实施严格、有效地口令管理措施。

（2）对口令使用者进行培训，增强其安全意识。

（3）定期更新口令。

（4）确保口令的使用者的唯一性。

（5）严格限制从一个口令认证终端一次连续针对同一口令的认证次数。

（6）及时更改系统预设的口令。

口令系统的设计必须与具体应用环境的安全认证要求相结合。一般地，通过在口令系统中的使用方和验证方中采用单向函数，可以在一定程度上防范线路窃听、对付验证者攻击和对付重放攻击。

一次性口令认证是口令认证的特殊形式。它通过采用随机口令和同步技术确保任何两次认证中使用的口令都不相同，能够有效防范口令重放攻击。

生物特征识别也是一种非密码的认证方式。目前可以采用的生物特征主要有：指纹、声音、虹膜、视网膜、手形、面部等。其中，指纹识别技术、声音识别技术和虹膜识别技术的发展相对成熟，已经被用于一些认证环境，例如门禁、网上银行等。其他几类生物特征识别技术的使用目前仍相当有限。但是，由于生物特征识别具有其他认证机制不具备的优势，例如使用的方便性（无需携带或保存专门的认证信息）、严格的唯一性等，它具有很好的应用前景。

3.4 授权技术

3.4.1 作用

目前我们所见到的授权技术，主要是为应用（包括用户和应用程序）提供针对各种资源的授权管理和访问控制服务的技术。例如，访问控制列表等常见的访问控制技术都属于授权技术的范围。由于在真正的应用中，这些授权技术往往被解决方案的设计者加以综合运用，因此通常称为“授权管理基础设施（PMI）”。

由于 PMI 将针对应用系统资源的访问控制权限交由授权机构进行统一管理，它所实现的访问控制机制与实际应用的处理模式相对应，并且与具体应用系统的开发和管理模式无关。因此，PMI 能够极大地简化业务应用中权限管理和访问控制系统的开发与维护过程，降低管理工作的复杂性，降低管理成本。此外，通过将授权管理系统与身份认证系统相结合，PMI 补充了 PKI 的弱点，并提供了 PKI 与应用计算环境的二者间的集成模式。

使用 PMI 平台构建访问控制系统，能够极大地减少开发周期和开发费用。通过使用统一的管理界面，能够减少管理的复杂性，增加系统的可维护性，并可以根据应用的变化更改策略或定制新的策略，提高系统的适应性。但是，PMI 只是电子政务实现授权管理和访问控制服务的一种形式。在某些具体的电子政务建设与应用环境中，信息安全传统意义中的访问控制措施也能够提供此类服务，没必要构建 PMI。

3.4.2 基本结构和应用模型

PMI 的基本结构和应用模型如图 3-4-1 所示。

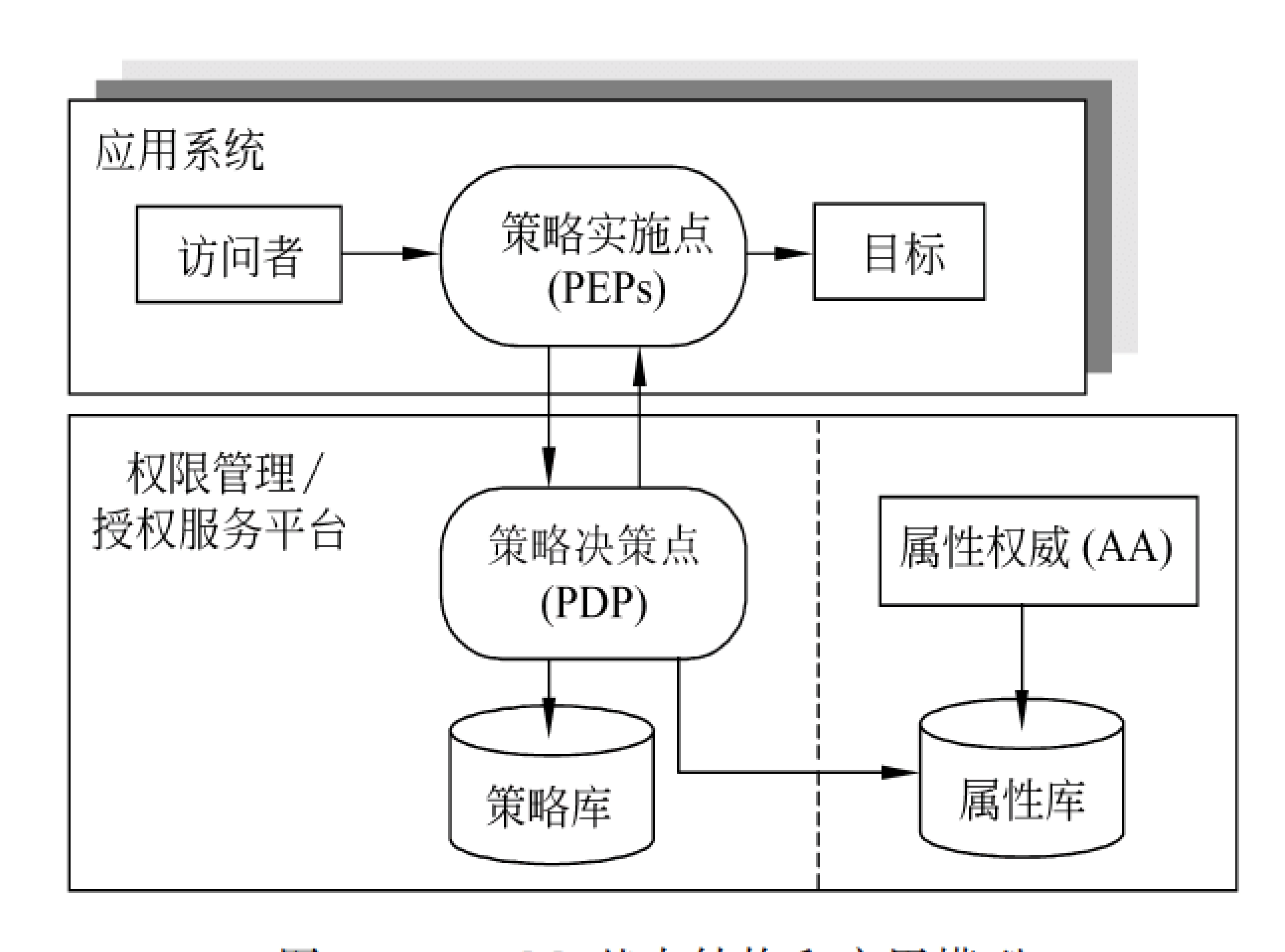


图 3-4-1　PMI 基本结构和应用模型

各组成部分的说明如下：

(1) 访问者和目标：均是实体(可以是人或其他计算机实体)。

(2) 策略实施点(Policy Enforcement Points，PEPs)：介于访问者和目标之间，指已经被接口插件或者代理修改过的应用或服务(这种应用或服务被用于实施一个应用内部的策略决策)。当访问者申请访问目标时，策略实施点向策略决策点申请授权，并根据授权决策的结果确定允许访问目标或拒绝访问。PEP 对每一个具体应用可能不同。在具体的应用中，它可能是应用程序内部中进行访问控制的一段代码、安全应用服务器(例如 Web 服务器及其上增加的一个访问控制插件)，或者安全应用网关。

(3) 策略决策点(Policy Decision Point，PDP)：又称授权策略服务器，负责接收和评价授权请求。它是一个通用处理逻辑，根据具体策略做出不同的决策，与具体的应用无关。当接收到一个授权请求时，它从策略仓库中获得策略数据，并依据策略逻辑、访问者的安全属性和当前条件进行决策，然后将决策结果返回给策略实施点。在具体应用中，策略决策点是一个判断逻辑，它可以与策略实施点结合在一起，也可以单独运行于一个独立

的服务器上。最简单的实现方式是：策略决策点根据访问控制列表（Access Control List，ACL）进行查表操作，判断用户的权限。

（4）安全授权策略说明授权遵循的原则和具体的授权信息。具体而言，策略包含应用系统中的所有用户信息、资源信息，以及这些信息的组织管理方式、用户和资源之间的权限关系、安全的管理授权约束、系统安全的其他约束。

（5）属性权威（Attribute Authority，AA）：属性证书（AC）的签发者。属性权威的根称为 SOA。

（6）属性库：实际是一个独立的 LDAP 服务器，主要用来存放属性证书和其他相关信息，并提供检索服务。

（7）策略库：主要用来存储安全授权策略数据、用户和资源信息，以及 PMI 所需的相关数据。策略库可以是一个数据库，也可以使用 LDAP 存放这些信息。对于某些应用，可以将 AA 签发的属性证书直接存放在策略库，并将属性库和策略库统称为策略库。

3.4.3 体系结构与主要功能

一般地，根据资源的具体特点和应用的实际需要的不同，授权管理基础设施的授权管理服务有两种工作模式：集中式与分布式。两种工作模式下的授权管理系统应该支持 X.509 v4 属性证书格式。

1. 集中式授权管理服务系统

集中式授权管理服务系统基于相对固定的授权模型，提供集中式管理，通过在数字证书的扩展项中增加用户的属性或权限信息，在服务器端构建授权管理（Privilege Management，PM）服务系统提供授权管理。PM 服务系统提供用户管理、审核管理、资源管理和角色管理。

集中式授权管理服务系统主要特点是权限独立下载至用户公钥证书中，即 CA 和属性权威（AA）紧密结合在一起，权限代码/权限属性嵌入公钥证书的扩展项中。

该系统的体系结构如图 3-4-2 所示。

（1）授权管理模块：完成资源访问授权、撤销授权、授权委托。

（2）授权信息目录服务器：发布授权信息。

（3）资源管理模块：接收用户请求，验证用户的数字证书，向策略引擎发出访问控制判断请求，将访问控制列表提交给策略引擎。

（4）策略引擎：根据资源管理模块的请求，访问授权信息目录服务器，取得用户的授权。根据资源的访问控制列表和用户的授权，做出访问控制判断。

（5）密码服务系统：提供基础的密码服务，主要包括加解密、数字签名、数字信封等。

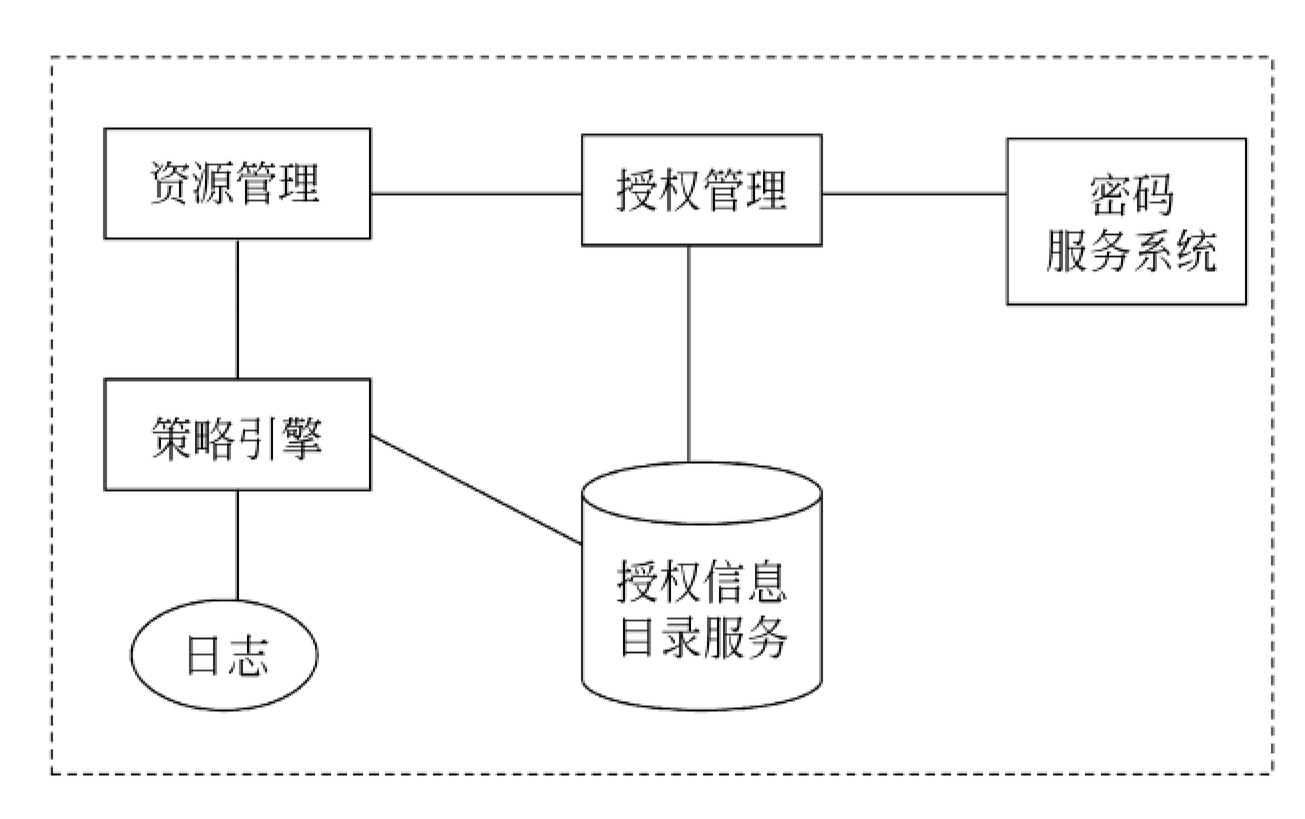


图 3-4-2　集中式授权管理体系结构图

集中式权限管理服务系统的主要功能是：用户管理、审核管理、资源管理、角色管理、操作员管理和日志管理。

(1) 用户管理：提供管理用户信息功能，包括用户注册、用户信息修改、用户注销。

(2) 审核管理：主要完成用户授权申请的审核功能。

(3) 资源管理：制定资源访问控制列表，即根据实际的应用，把资源和用户角色关联起来，标识用户角色对资源的访问权限。

(4) 角色管理：包括角色的制定、编辑、更新。根据具体应用实际，制定出恰当的角色信息，以便和用户的实际身份相映射。权限管理中心制定出完整的角色信息，并把角色信息同步到资源管理中心。

(5) 操作员管理：功能包括增加操作员、注销操作员、操作员权限设置、修改操作员权限等。

(6) 日志管理：对操作员的所有操作活动等信息进行日志记录。日志管理的功能包括日志参数设置、日志查询、日志备份。

2 分布式授权管理服务系统

分布式授权管理服务系统采用灵活的授权方式，提供分布式管理服务，通过在客户端根据用户具体情况进行个性化定制，灵活设置有效地授权信息，由资源所有者自行分配资源的访问权限，并通过采用数字签名技术使授权信息具备不可否认性。

在分布式授权管理服务系统中，权限同样独立下载至用户公钥证书中，但该系统与集中式授权管理服务系统的不同点在于：以业务应用系统划分权限管理域，属性权威(AA)把用户权限证书独立地下载于用户的公钥证书载体上，由不同业务应用系统分别签发、下载本系统的权限证书。

该系统的体系结构如图 3-4-3 所示。其中，各组成部分的作用分别是：

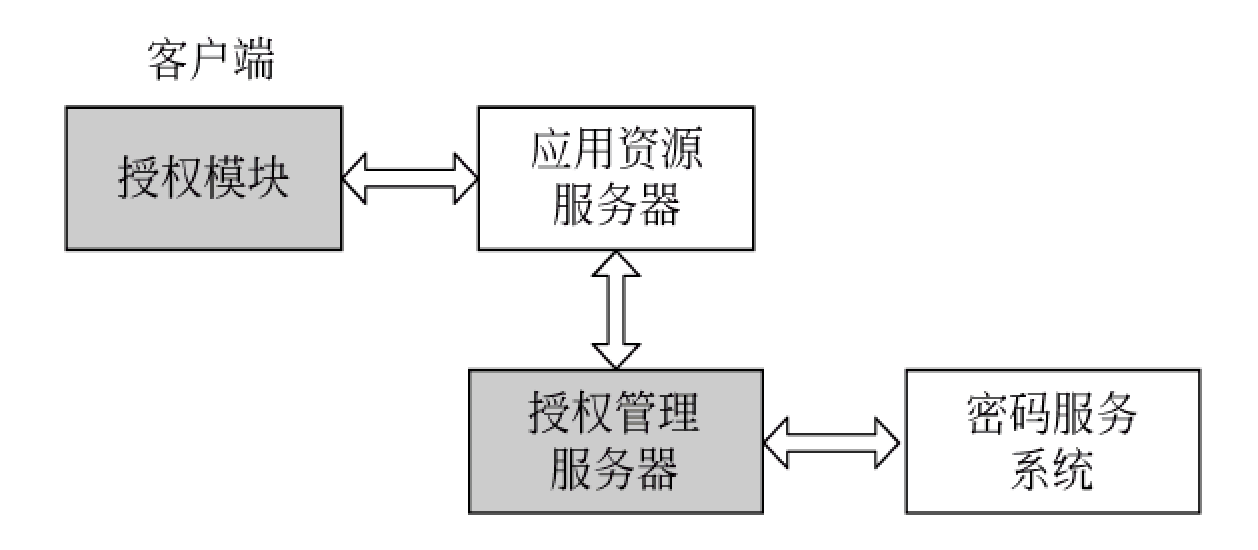


图 3-4-3 分布式授权管理体系结构图

(1) 客户端授权模块：完成用户对资源的个性化授权并签名。

(2) 应用资源服务器：接收访问请求，并向授权管理服务器发出访问授权请求。

(3) 授权管理服务器：存储资源的授权信息，接收应用资源服务器的请求，根据资源的访问授权，计算访问权限值并将该值返回给应用资源服务器，同时提供相应的资源管理功能。

(4) 密码服务系统：提供基础的密码服务，主要包括加解密、数字签名、数字信封等。

分布式授权管理服务系统的主要功能是：资源访问授权、操作员管理、权限管理、日志管理。

(1) 资源访问授权：根据用户的资源授权信息等数据制定访问授权列表，并完成用户对列表的签名。

(2) 操作员管理：功能包括增加操作员、注销操作员、操作员权限设置、修改操作员权限等。

(3) 权限管理：包括授权更改和授权删除。授权更改完成对用户制定的授权信息列表修改功能；授权删除完成对授权信息进行删除的功能。

(4) 日志管理：对操作员的所有操作活动的时间、事件等信息进行日志记录。日志管理的功能包括：日志参数设置、日志查询、日志备份。

例如，汉邦安全授权管理系统就采用了分布式架构，通过引进协同机制对网络系统中的主机、服务器、网络进行分级和全方位的授权管理，从而实现了对网络资源、信息资源进行全方位的管理和维护，并实现了对重要数据的保护、对用户行为授权，以及对网络设备、网络性能、故障等进行分析、审计等管理工作。

3.4.4 性能指标

一般地，就性能指标而言，授权管理基础设施对应用层的服务器端和客户端的密码设备的性能指标不同。其中，应用层的服务器端密码设备应达到如下性能指标：

(1) 公钥密码算法签名速度≥2000 次/s。

（2）公钥密码算法验证速度≥16 000 次/s。

（3）对称密码算法加解密速度≥500Mb/s。

（4）可存储的密钥对≥64 对。

应用层的客户端密码设备应达到如下性能指标：

（1）公钥密码算法签名速度≥2 次/s。

（2）公钥密码算法验证速度≥16 次/s。

（3）对称密码算法加解密速度≥100Kb/s。

3.5 容灾备份与故障恢复技术

3.5.1 作用

容灾备份包括系统备份和数据备份。容灾备份通常采取本地备份和异地备份这两种方式实现。容灾备份与故障恢复技术的目标是：确保应用系统、关键数据具有很强的稳定性与可靠性。在灾难或故障发生后，仍然能够维持正常运行或及时恢复，确保系统或关键数据的可用性。

3.5.2 体系结构

为了应对各种可能出现的灾难和故障，容灾备份和故障恢复系统必须依据安全策略，采取多种措施相结合。

（1）本地备份：本地系统关键设备的双机热备份，本地系统关键数据的冷备份。

（2）异地备份：异地备份中心。

（3）系统恢复。

（4）数据恢复。

容灾备份与故障恢复系统的体系结构如图 3-5-1 所示。

其运作过程如下：

（1）正常情况下，业务处理只在主中心运行；业务系统对数据的任何修改，实时同步地复制到备份中心。

（2）当主中心的某些子系统发生故障时，系统会自动地快速切换到主中心的其他设备，确保系统正常运行。

（3）当灾难发生，导致主中心整个系统瘫痪时，能实时监测到这种异常情况，及时向管理员发送各种警报，并按照预定的规则在备份中心启动整个业务应用系统。

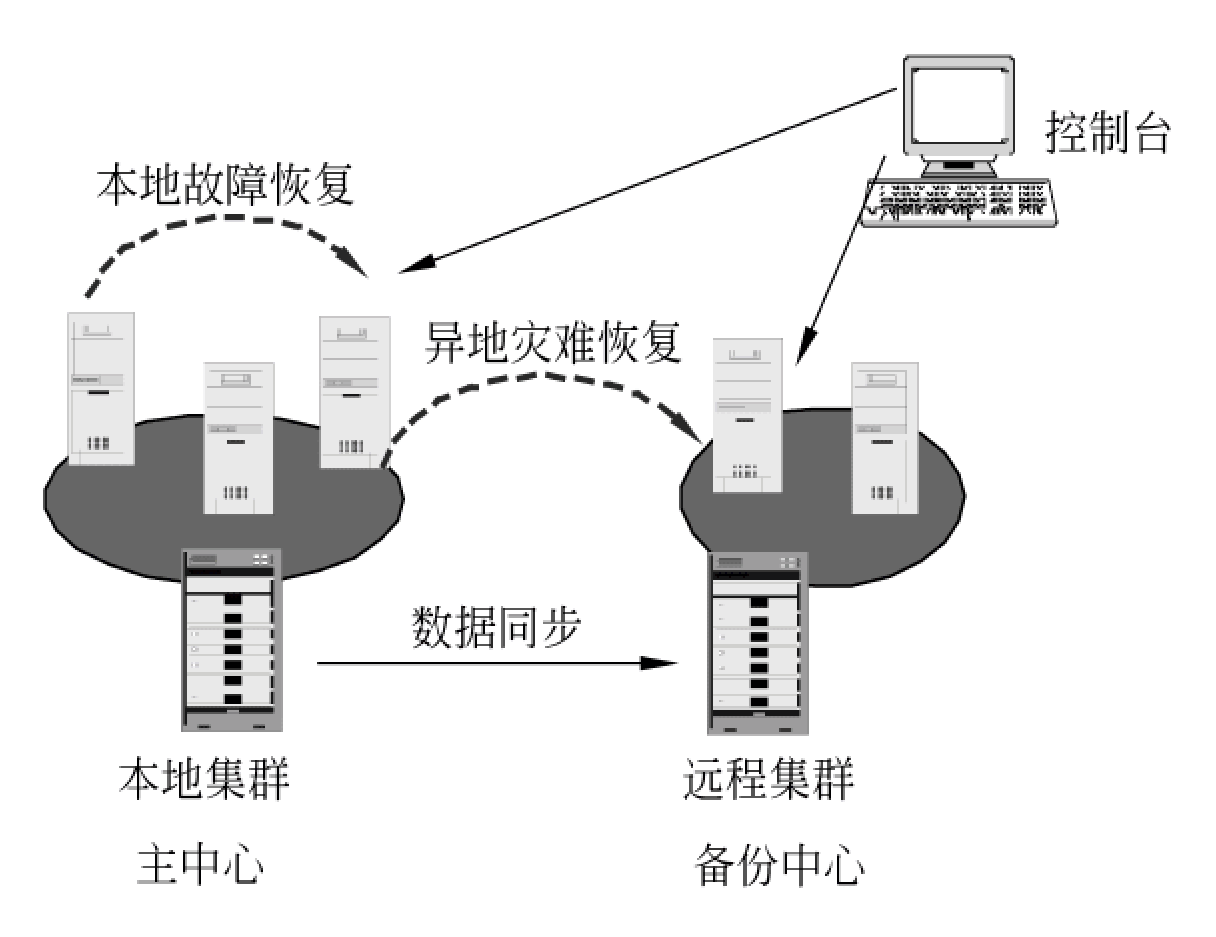


图 3-5-1　容灾备份与故障恢复系统体系结构图

（4）主中心系统修复后，可将备份中心的当前数据复制回主中心，然后将业务处理从备份中心切换回主中心，备份中心重新回到备份状态。

3.5.3　容灾备份的策略

制定具体的备份策略需根据各种应用和业务处理的特点，并遵循以下原则：

（1）对所有关键的应用，应至少保证各种必要的热备份机制，包括双机热备、磁盘镜像等。

（2）对于所有应用，应提供磁带备份和恢复机制，保证系统能根据备份策略恢复至指定时间的状态。

（3）对于操作系统和应用程序代码，在每次系统更新或安装新软件和做一次全备份。对于一些日常数据更新量大，但总体数据量不是非常大的关键应用数据，可每天在用户使用量较小的时候安排全备份。对于日常更新量相对于总体数据量较小，而总体数据量非常大的关键应用数据，可每隔一个月或一周安排一次全备份，在此基础上，每隔一个较短的时间间隔做增量备份。

（4）对一些关键数据，预先定义备份窗口大小，再根据备份数据量计算所需的备份速度。

（5）保存有过时数据的介质可重新覆盖使用，轮换频率可根据备份类型和备份的要求来确定。

（6）根据介质容量、全备份、增量备份和每种介质的保留时间或轮换频率计算出所需的介质数目。

（7）备份好的介质，要放到保险柜或运输到备份中心统一保存。为了更好地管理介质，对所有磁带需按统一的规则来命名。

3.5.4　本地备份

本地备份包括系统备份和数据备份。系统备份包括设备硬件备用和软件备份。

在设备的使用过程中，由于不可抗力和硬件设备本身的使用寿命有限，设备难免会发生故障或损坏。为了及时应对这类故障，必须依据具体的应用需求建立一套硬件设备备用机制。

此外，可以利用有关软件将整个硬盘备份成一个镜像，在系统被严重破坏时，就可以很快把资料完全复原。因此，可以将刚安装好应用程序的系统做一个备份的映像，以后安装系统只要极短时间就可以完成，达到快速恢复系统的目的。

数据备份是确保重要数据不丢失和具有抗毁性的最主要措施。数据备份的目的是：

（1）对网络内部的重要业务资料进行自动化存储管理。

（2）简化备份复杂性，节省人力资源，提高工作效率。

（3）确保数据存放安全，并有效集中管理。

（4）避免人为错误及自然灾害的破坏，提高数据资料的正确性。

（5）缩短备份/恢复工作的时间。

（6）协助实现异地备份/恢复、系统灾难恢复。

数据备份有三种类型：

（1）完全备份：定期对系统中每个数据库文件制作备份。

（2）特别备份：在系统进行大的改动后进行的备份。

（3）增量备份：在系统的日常应用中，只对系统新增数据进行备份，即只备份上次全盘备份之后更改过的所有文件。

数据备份的实现方式主要有以下三种，可以根据具体业务的应用情况进行选择。

1）磁盘阵列

在磁盘阵列上以容错机制对数据进行镜像保存。当镜像硬盘发生故障时，管理员应该能够在不中断数据访问的前提下，以在线方式更换磁盘硬件。随着系统应用的演进和数据量增长的需要，如果在现有盘阵的基础上增加新的硬盘或阵列，同样应该能够以在线方式完成对文件系统的容量调整和性能调整。

2）磁（光）介质备份/恢复系统

磁（光）介质备份是指用磁带（或可刻写光盘）对数据资料进行可靠的备份。一般地，这种备份是对所有的数据进行集中式的定期备份。备份应该一个全自动化进行的过程，并且可以选择通过自动化的硬件（如带机械手的磁带库）来完成。对于备份软件而言，应在识别数据库的数据结构的基础上，避免不必要的人工干预（如 export 形成中间文件等），直接对数据库数据进行备份。此外，针对不同时期的数据内容变化，可以采用增量备

份的办法实现。

3）本地双机热备份系统

即使用容错方式保证了磁盘阵列系统的高可用性，主机系统的可靠性仍不容忽视。为了避免主机系统中存在单点故障，需要用两台主机形成集群环境，保证其高可靠性。支持集群环境的软件应该能够识别单一的主机故障，并能够在极短的时间内将故障主机上运行的应用程序以及数据库切换到备用主机上。同时，集群软件应该能够将故障主机的IP服务地址迁移到备用主机，以便所有的客户机能够继续使用原来的IP地址对数据库进行访问。

数据备份系统应该具备两个特点。首先，该系统应该在灾难发生情况下进行快速可靠的数据恢复操作，尽可能地减少管理和人员成本、提高效率。其次，该系统应该具有很好的伸缩性，能够在不断更新系统数据的过程中进行方便、高效、可靠的扩展。

3.5.5 异地备份

异地备份的主要实现方式是设立异地备份中心。该中心不仅要实现本地的切换保护外，更要实现数据的实时异地复制，以及业务系统（包括数据库和应用软件）的实时远程切换。

例如，一般的电子政务应用为了对重要数据进行安全备份，需要在部、省两级建立数据备份中心。部级数据备份中心应在适当的地域建设灾难备份中心。有条件的省份也应在省内建设相应的灾难备份中心。同时，有条件的省份还必须建立数据备份中心，集中备份全省范围内的数据。那些没有条件建立集中的数据备份中心的省份，可将数据分散在省内存放，同时尽可能地将数据集中地备份到部级备份中心。

异地备份中心的建立需要满足的要求主要有：

（1）备份中心与主中心之间的距离不小于500km。

（2）备份中心具备足够的网络带宽，以便确保与主中心的数据保持同步。

（3）备份中心要有足够的处理能力，以便成功接管主中心的业务。

（4）备份中心与主中心的应用切换必须快速可靠。

3.5.6 恢复

为保证应用系统具有最高程度的可靠性，必须建立故障恢复系统，包括系统恢复和数据恢复。此外，在必要的情况下，还应该通过高速的网络专线实现对信息网络中心数据的远程复制，即建立远程灾难恢复系统。这样，当主系统不能正常运转时，恢复系统的远程监控软件能够及时识别故障情况，并且能够根据不同业务的特点，自动地将故障系统上的数据库业务转移到备份系统环境中正常运行。

故障恢复包括系统恢复和数据恢复。

对关键应用系统，必须能够有效规避任何单点故障，以便确保在发生上述故障的情况下系统依然能够正常运转。这些故障包括：应用程序错误、数据库系统故障、网络端口故障、网线接入故障、磁盘系统介质故障、系统瘫痪等。

系统恢复的措施主要有：

(1) 群集配置：由多台计算机组成集群结构，尽可能消除整个系统可能存在的单点故障。

(2) 双机热备份：在任何一台设备失效的情况下，按照预先定义的规则快速切换至相应的备份设备，维持业务的正常运行。

(3) 磁盘镜像：部署两台服务器，通过光纤连接其共享的磁盘阵列，实现主机系统到磁盘系统的高速连接。

(4) 故障恢复管理：由专门的集群软件进行管理和监控，使应用系统在任何软硬件组成单元发生故障时，能够根据故障情况重新分配任务。

数据恢复需要考虑的两个关键因素是数据恢复的过程和数据恢复所需的成本。

数据恢复过程涉及参与人员、管理制度和操作规程。它们的具体内容需要依据应用需求来确定。其中，参与人员通常是评估经理、系统集成项目经理、安全设计师、安全顾问和客户服务工程师。

数据恢复所需的成本主要和进行数据恢复操作的时间代价与空间代价有关。

在时间代价方面，一般地，目录数据恢复和普通数据恢复需要的时间不同。对于复制目录而言，其成本与操作方式直接相关。可以从备份介质中对目录数据实现冷恢复。空间代价主要与需要恢复的数据量有关。

3.6　恶意代码防范技术

3.6.1　防范策略

由于近年来恶意代码破坏性不断增加，危害性大，影响范围广，以及病毒、蠕虫、黑客程序等恶意代码又有相互融合的趋势，病毒防治已经不是一项简单的任务，而是需要依据整个网络的体系结构来制定相应的解决方案。一般地，建议采用集中控制、分级管理、多层防护的体系结构，为应用系统提供统一的病毒防护和监控服务。这样，不仅可以减轻管理员的工作负担，还可以确保广域网中每一台计算机（包括服务器和客户端）具有相同的防病毒能力。由于计算机病毒在恶意代码中最为传统，截至目前，很多恶意代码防范技术

以及相关产品仍然被称为“防病毒技术”、“防病毒软件”。但事实上，他们的外涵已经涉及了蠕虫、黑客程序等更多种类的恶意代码。因此，本书也将恶意代码简称“病毒”。

集中控制、分级管理、多层防护的具体含义分别是：

集中控制：指各级管理中心负责本级系统的防病毒工作，以各级管理中心为防病毒控管中心，对本级系统各个部分进行集中控制，实时监测全网内的病毒情况。

在全网范围内，各级系统实施统一的防病毒策略（包括同时更新病毒定义码和扫描引擎，根据实际情况及时调整防病毒策略和力度等）。

分级管理：指各级管理中心负责管理所辖区域内的病毒防治工作，并定期向上级管理中心汇报。

多层防护：指各级防病毒管理中心从网关、服务器到客户端层层设防，防止病毒的传播和扩散。

一般地，可以从以下三个层次实施恶意代码防范：

1）网络边界防护

在网络边界（例如网关）处进行病毒过滤和防护。这是阻止病毒入侵网络的最有效措施之一。因为病毒主要是通过 SMTP、HTTP、FTP 三个协议通道进行入侵，需要针对这三个协议进行内容扫描和杀毒。

2）集群服务器/邮件系统防护

集群服务器是办公的基本平台，很容易成为病毒的集中地。目前，市场上主要的集群服务器是 Lotus Domino/Notes 和 Microsoft Exchange。由于集群服务器往往采用特有的内部协议进行工作，需要使用针对每种系统对应的防毒软件，帮助实现对整个集群系统的全面保护。

3）主机病毒防护

在各个主机系统上安装防病毒软件并定期升级。

此外，必须通过以下方式对应用系统病毒定义码和扫描引擎进行更新、升级：

（1）对各级管理中心防病毒服务器，采用升级工具与生产厂商病毒库连接，对病毒定义码和扫描引擎进行更新、升级，然后再将其分发给各自的下属部门。

（2）由管理网络中心统一更新、升级病毒定义码和扫描引擎，各子系统要到相应的上级管理中心进行升级工作。这样，一方面可以确保同级系统病毒定义码和扫描引擎的更新基本保持同步，支持整个系统具有很强的防病毒能力。另一方面，整个网络的病毒定义码和扫描引擎的更新、升级自动完成，可避免由于人为因素造成网络中某些机器或某个网络因为没有及时更新病毒定义码和扫描引擎而失去病毒防护能力。

3.6.2　功能要求

本节主要介绍病毒查杀、网关防毒系统、群件防毒系统和集中管理系统的基本功能要求。

1. 病毒查杀系统

病毒查杀的基本功能要求是：

（1）实时病毒查杀的能力。

（2）对已知病毒完整的查杀能力。

（3）对未知病毒强大的清查预警能力。

（4）在网络的各个结点处，如网关、群件系统、服务器和个人机上，都能提供相应的病毒查杀能力。

（5）对受感染的系统能够提供病毒清除和系统恢复能力。

（6）防病毒产品应通过指定机构的权威检测认证，并获得销售许可证。

2. 网关防毒系统

网关防毒系统的基本功能要求是：

1）高度的稳定性

在网关处的防毒系统需要高度的稳定性。产品应提供 24 小时不间断运行的能力，以保证整个网络的出口不受影响。

2）灵活的部署方式和能力

网关防毒系统能够支持各类复杂的网关环境和平台，能够与诸如防火墙、代理服务器、邮件网关等设备的协作能力。

3）附带内容过滤和紧急处理能力

网关的紧急处理能力是指使用内容过滤技术，在从病毒出现到防毒厂商送出新的病毒码这段“空窗期”内，对可疑内容实行紧急隔离措施，以保证整个网络在第一时间将新病毒拒之门外，或是抵御 DDOS 攻击。

4）可扩展性和可管理性

防毒系统应该随硬件平台的升级而动态扩展自身的处理能力，还应能支持诸如负载均衡和群集的能力，具有良好的可扩展性。

5）管理界面

应支持目前普遍的 Web 应用方式，方便和简化管理员的操作。

6）其他

对于病毒查杀情况，应有完整的日志记录，以及可选的各类通告或报警机制。此外，

由于 SMTP 和 HTTP 协议传输内嵌可执行内容，经常造成用户在接收到信息的同时遭到病毒的入侵和感染，部署网关防毒系统时需要重点考虑保护 SMTP 和 HTTP 协议传输内容。相对地，因为通过 FTP 传输的内容则完全由用户控制其后续动作，客户端的防毒系统很容易检查出此类病毒，这类内容通常不是网关防毒系统关注的重点。

3. 群件防毒系统

群件防毒系统的基本功能要求是：

1）稳定性

群件系统作为业务应用（尤其是办公自动化应用）的核心系统，其不间断运行能力至关重要，要求相配套的防毒系统应具有极强的稳定性。

2）占用较低的系统资源

一般地，群件防毒系统直接安装在集群服务器上，需要避免在防毒的同时过多地占用系统资源，否则可能会导致群件服务本身无法正常或良好地运转。

3）具备内容过滤和紧急处理能力

类似于起到网关的紧急处理作用。如果群件防毒系统有类似这样的模块，可以在第一时间阻止来自内外网的新病毒入侵和 DDOS 攻击，从而保护群件服务器的正常运作。

4）完整的保护

防毒系统应该针对集群服务器的特点，提供从邮件传输、文件及数据库共享、数据复制等各个过程的实时保护功能，确保整个系统的安全性。

部署前应检查服务器自身系统资源的使用情况，必要时需对各部分的资源配置进行扩展。

4. 集中管理系统

集中管理系统的基本功能要求是：

1）全面的集中管理和监控功能

该系统应能对从网关到客户端的各个防毒系统结点进行统一的管理和监控，从而让管理人员真正做到对整个网络内防毒系统的单点监控。

2）单点下载，自动更新部署功能

该系统应该能够在管理系统的单点上更新最新的病毒码、杀毒引擎，甚至是程序的更新版本，然后将其自动部署到网内所有的防毒系统上。

3）集中的日志和报警功能

集中的日志为监控和跟踪整个网络的病毒情况提供了有效地途径。集中的报警功能对分次发现的大量病毒报告进行过滤，只在某段时间内病毒出现达到一定数量时才报警，帮助管理员对病毒爆发的情况做出反应。

3.7 入侵检测技术

3.7.1 作用

1980 年，James Anderson 首先提出了入侵检测的概念，将入侵尝试（intrusion attempt）或威胁（threat）定义为：潜在的有预谋未经授权访问信息、操作信息、致使系统不可靠或无法使用的企图。他还提出审计追踪可应用于监视入侵威胁。1987 年，Dorothy Denning 提出入侵检测系统的抽象模型，首次将入侵检测的概念作为一种计算机系统安全防御问题的措施提出，与传统加密和访问控制的常用方法相比，入侵检测方法成为全新的计算机安全措施。

在此以后随着计算机网络的发展，以及大规模网络安全事件的爆发，入侵检测技术作为信息安全中重要的组成部分得到很大的发展，相继出现了一系列系统与模型。例如，为检测用户对数据库的异常访问在 IBM 主机上用 COBOL 开发的 Discovery 系统；入侵监测模型、入侵检测专家系统（Intrusion Detection Expert System，IDES）、与系统平台无关的实时检测思想、1990 年基于网络的入侵检测——NSM（Network Security Monitor）的出现，以及后来的分布式、协同处理入侵检测技术的发展；近年来将免疫原理和信息检索技术引入入侵检测等。

入侵检测是指通过从计算机网络或计算机系统中的若干关键点收集信息并对其进行分析，从中发现网络或系统中是否有违反安全策略的行为和遭到攻击的迹象，同时做出响应。

入侵检测系统（Intrusion Detection System，IDS）是实现入侵检测功能的一系列的软件、硬件的组合。入侵检测系统以实时方式监测网络通信，对其进行分析并且进行实时的安全预警，从而能够有效地管理内部工作人员安全地使用内部资源，并对外部的攻击进行早期预警和跟踪，有效地保障系统安全。因此，需有专用的入侵检测设备或入侵检测软件进行监测，及时采取相应的安全措施遏制入侵行为。

入侵检测的主要功能有：监测分析用户和系统行为、审计检查系统配置和漏洞、重要系统和数据文件的完整性评估、已知的攻击行为模式的识别、异常行为模式的统计分析、操作系统的审计跟踪管理及违反安全策略的用户行为的识别、对入侵行为做出紧急响应。

通过开发一些协议和应用程序接口，入侵检测系统组件也可以被其他系统应用。

3.7.2 CIDF 定义的入侵检测系统构件

为了解决不同入侵检测系统的互操作性和共存问题，有学者提出了通用入侵检测框

架(Common Intrusion Detection Framework,CIDF),对入侵检测进行标准化工作。CIDF主要是通过定义数据格式和数据交换接口来实现其目标,并没有对IDS的体系结构进行任何约束,也没有限制实现所采用的编程语言和操作系统。它将IDS的构成划分为5类构件:事件构件、分析构件、数据库构件、响应构件和目录服务构件,如图3-7-1所示。

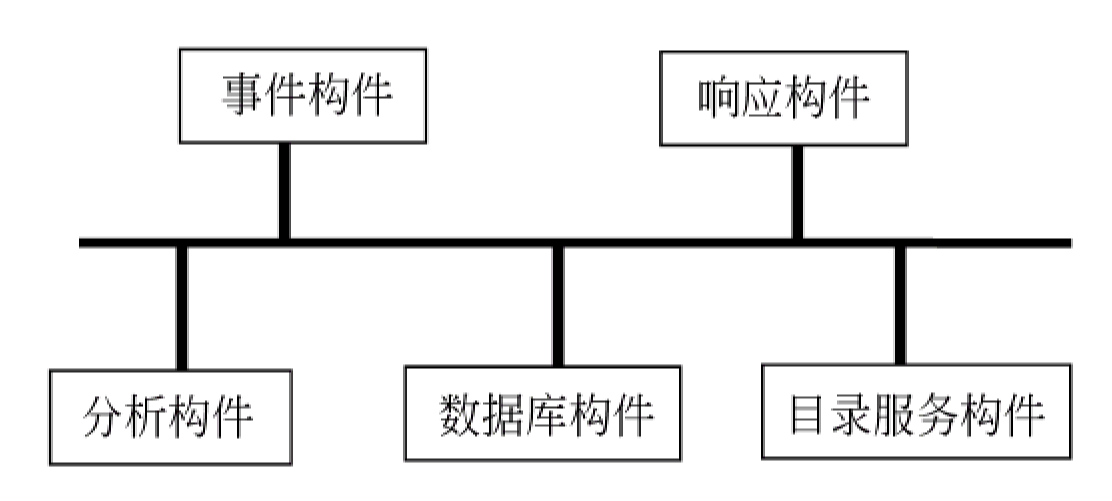


图 3-7-1　IDS系统构件模型图

其中,各构件的作用分别是:

(1) 事件(event)构件:整个计算环境中获得事件,并向系统的其他部分提供此事件具备一定的数据过滤功能。

(2) 分析(analyze)构件:分析事件数据,以及其他各构件的数据信息,根据数据分析确定应该采取的行动。

(3) 数据库(databases)构件:对系统各个阶段的数据进行管理,在IDS中,数据量很大,数据的动态性也很强,同时因为考虑到系统的处理层次需要将数据用多种形式缓存,所以必须有一个数据库构件来缓存数据。

(4) 响应(response)构件:对分析结果做出反应的功能单元,它可以做出切断连接、改变文件属性等强烈反应,也可以只是简单的报警。

(5) 目录服务(directory serve)构件:它用于各构件定位其他构件,更重要的是控制其他构件传递的数据并认证其他构件的使用,以防止IDS本身受到攻击。目录服务构件可以管理和发布密钥,提供构件信息和告诉用户构件的功能接口。

3.7.3 分类

一般地,我们将入侵检测系统分为基于主机的入侵检测系统、基于网络的入侵检测系统和基于代理(agent based)的入侵检测系统。

(1) 基于主机的入侵检测系统通常以系统日志、应用程序日志等审计记录文件作为数据源。它是通过比较这些审计记录文件的记录与攻击签名(attack signature,指用一种特定的方式来表示已知的攻击模式)以发现它们是否匹配。如果匹配,检测系统就各系统管理员发出入侵报警并采取相应的行动。基于主机的IDS可以精确地判断入侵事件,并

可对入侵事件做出立即反应。

(2) 基于网络的入侵检测系统把原始的网络数据包作为数据源。它是利用网络适配器来实时地监视并分析通过网络进行传输的所有通信业务。它的攻击识别模块进行攻击签名识别的方法有：模式、表达式或字节码匹配；频率或阈值比较；次要事件的相关性处理；统计异常检测。一旦检测到攻击，IDS 的响应模块通过通知、报警以及中断连接等方式来对攻击行为做出反应。然而它只能监视本网段的活动，并且精确度较差，在交换网络环境中难以配置，防欺骗的能力也比较差。网络入侵检测系统的主要功能要求有：

- 支持异常检测与统计检测等检测方法；
- 检测模块与特征库能够扩充和进行在线升级；
- 自动识别多种类别的攻击行为；
- 能够支持自定义策略；
- 支持集中式的安全监控管理；
- 支持管理、监视、控制和分析功能相融合的图形化控制台；
- 具有多种实时报警和响应手段，可以通过网络、有线、无线等多种方式向系统管理员发布报警信息；
- 在日志中记录所有的报警事件；
- 具有事件分类显示功能并支持组合搜索分析。

(3) 基于代理的入侵检测系统用于监视大型网络系统。随着网络系统的复杂化、攻击行为也表现为相互协作式特点，所以不同的 IDS 之间需要共享信息，协同检测。整个系统可以由一个中央监视器和多个代理组成。中央监视器负责对整个监视系统的管理，代理则被安放在被监视的主机上负责对其活动进行监视，然后将获取的数据传送到中央监视器。

另外，根据采用的检测方法不同，可将入侵检测技术分为异常入侵检测技术(anomaly detection)和误用入侵检测技术(misuse detection)。

(1) 异常入侵检测也称为基于行为的检测，其基本思想是：假定所有的入侵行为都是异常的。首先建立系统或用户的“正常”行为特征轮廓，通过比较当前的系统或用户的行为是否偏离正常的行为特征轮廓来判断是否发生了入侵。异常检测是一种间接的方法。

常用的具体方法有：统计异常检测方法、基于特征选择异常检测方法、基于贝叶斯推理异常检测方法、基于贝叶斯网络异常检测方法、基于模式预测异常检测方法、基于神经网络异常检测方法、基于机器学习异常检测方法、基于数据采掘异常检测方法等。对这些方法而言，需要重点解决的问题是特征量的选择和参考阈值的选定以确保虚警(false positives)和漏警(false negatives)尽量少发生。

(2) 误用检测也称为基于知识的检测，其基本思想是：假定所有可能的入侵行为都

能被识别和表示。首先对已知的攻击方法进行攻击签名(攻击签名是指用一种特定的方式来表示已知的攻击模式)表示,然后根据已经定义好的攻击签名,通过判断这些攻击签名是否出现来判断入侵行为的发生与否。这种方法是直接判断攻击签名的出现与否来判断入侵的,是一种直接的方法。

常用的具体方法有:基于条件概率误用入侵检测方法、基于专家系统误用入侵检测方法、基于状态迁移分析误用入侵检测方法、基于键盘监控误用入侵检测方法、基于模型误用入侵检测方法。对于这些方法而言,需要重点解决的问题是攻击签名的正确表示。

通常,入侵检测系统中的入侵行为分析模块应该具备以下功能:

- 支持集中的攻击特征和攻击取证数据库管理;
- 支持攻击特征信息的集中式发布和攻击取证信息的分布式上载;
- 提供对监视引擎和检测特征的定期更新功能;
- 能够划分安全等级,对网络系统进行安全检测和风险控制;
- 能够针对不同层次的人员提供不同层次的安全报告;
- 能够定期升级,确保系统在最短的响应时间内提出针对新的攻击和入侵方法的防范措施。

值得一提的是,IDS 已经逐渐向 IPS(入侵防御系统)过渡。国外已经从 2003 年开始陆续推出了 IPS 产品,而把 IDS 功能当作 IPS 运行时可选的一种模式,从而 IPS 逐渐替代了 IDS,成为入侵检测类产品的主打产品。IPS 是对 IDS 的包容和覆盖,同时具备了像防火墙一样的保护能力。IPS 可以有效解决与防火墙联动时延的问题,减少联动产生的副作用。

3.8 安全接口与中间件技术

3.8.1 作用

中间件是一种独立的系统软件或服务程序,位于客户机/服务器的操作系统之上,管理计算资源和网络通信。分布式应用软件能够借助中间件在不同的技术之间共享资源。

中间件的作用主要体现在以下三方面:

(1) 在分布式的客户和服务之间扮演着承上启下的角色,例如,实现事务管理、负载均衡以及基于 Web 的计算等。

(2) 屏蔽了低层操作系统的复杂性,减轻了应用软件开发者的负担,使他们能够面对一个简单而统一的开发环境,利用现有的硬件设备、操作系统、网络、数据库管理系统以及

对象模型,在创建分布式应用软件时减少程序设计的复杂性,避免了为程序在不同系统软件上的移植而重复工作。

(3) 保护企业的投资,保证应用软件的相对稳定,实现应用软件的功能扩展。

此外,由于分布式处理环境往往因为采用了多种多样的硬件、软件而具备相当的复杂性,而中间件产品能够在很大程度上降低这种复杂性程度,中间件正日益引起用户的关注。

安全中间件作为支撑软件,与应用系统的安全紧密相关,通常可以为应用与安全的整合提供先进的平台。目前,由于应用系统及其安全功能的复杂性,以及可持续性、可扩展性等现实要求,在体系设计与应用开发中采用中间件技术已经非常普遍。在关系到国家安全的系统开发与应用中,具有国内自主知识产权的安全中间件产品也已经成为首选。

一般地,安全中间件具备以下特点:

(1) 安全性高:具有自主知识产权和完备的安全构架。

(2) 透明度高:通过屏蔽复杂的安全技术,提供简易的应用层接口,使得应用系统开发人员无须具备专业的安全知识。

(3) 适应性强:使用多种标准语言实现,捆绑多种协议,支持目前广泛采用的应用架构、操作系统、安全协议、开发平台。因此,可以适应各种不同的应用环境。

(4) 可扩展性强:便于扩展新模块、捆绑新协议,而接口要相对稳定。

(5) 维护量小:采用先进的技术架构,保证了接口的稳定性,系统升级仅需更换部件,与安全集成的工作量主要集中在对安全中间件的升级上。

(6) 即插即用:支持各类应用系统与符合接口标准的安全设备无缝结合。

安全中间件采用层次化与模块化的设计体系,使应用与安全相分离,同时也使得各种安全服务相互分离。通过中间核心层的调度与管理,安全中间件能够实现应用与安全的有机结合,提供各个层次、满足各种需求的安全服务。

通常,安全中间件都捆绑了各种通用的安全协议,并且可与高层中间件相结合提供一体化的安全平台服务。

在实际应用中,具有自主知识产权以及完善的自身防护功能的安全中间件产品,在一定程度上已经具有可信计算平台的特点。此外,对于国外的安全中间件产品而言,通过将符合国际标准的安全服务模块更换成具有我国自主知识产权的模块,可以在应用系统的设计与开发中提高安全性。

3.8.2　体系结构

如图 3-8-1 所示,从体系结构上看,安全中间件通常由四层组成。

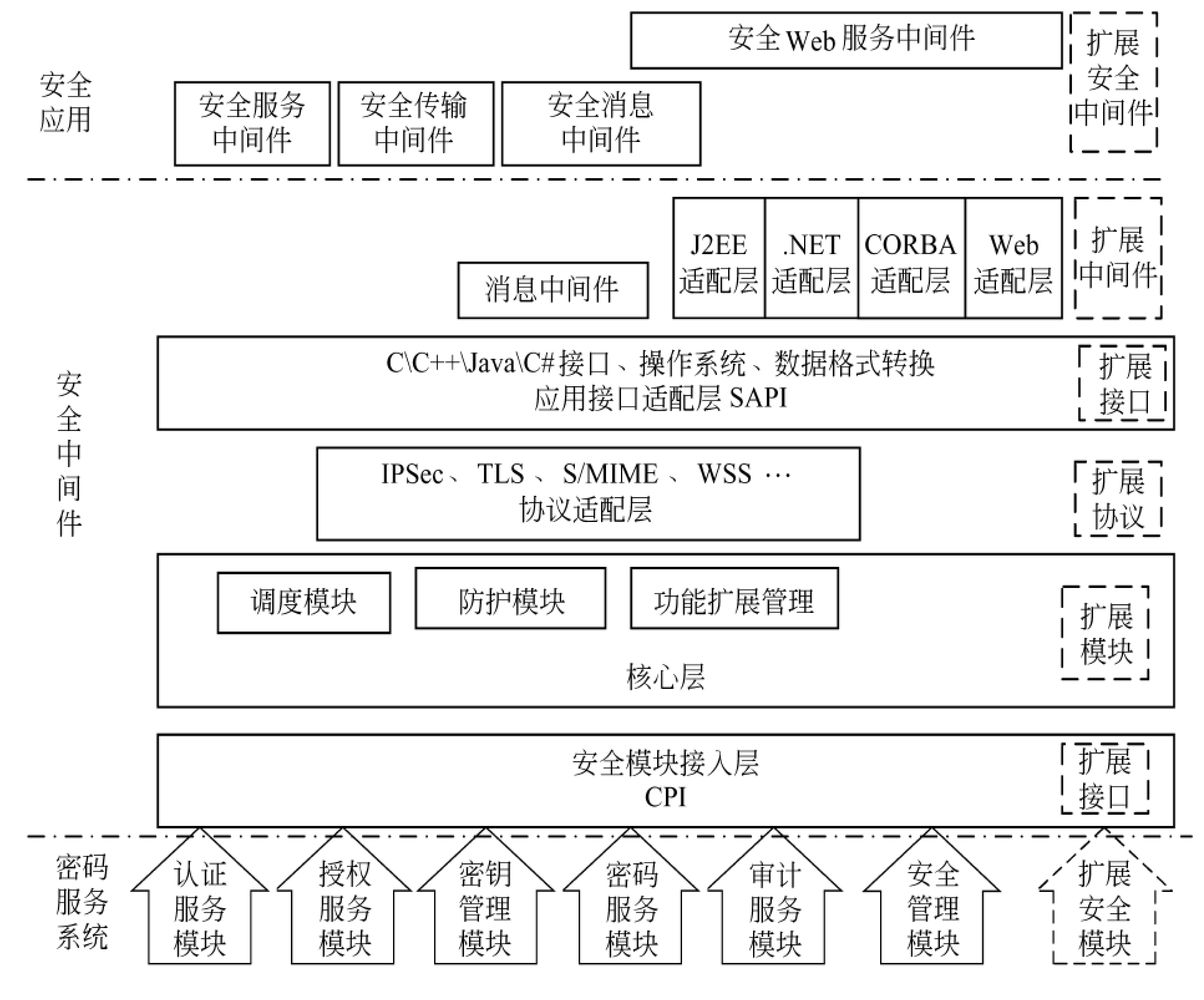


图 3-8-1 安全中间件体系结构

1. 安全模块接入层

安全模块接入层允许任何符合安全模块接口规范并通过认证的安全模块接入。

安全模块是由安全服务设备提供商提供的密码服务系统，如密码机、密码模块、便携式令牌等。安全模块包括：认证模块、授权模块、密钥管理模块、密码模块、存储模块、审计模块、安全管理模块等。各模块之间具有独立性。模块之间通过核心层的调度，可以实现互操作。例如，所有的模块必须支持密钥管理功能，而密钥管理服务由密钥管理模块统一提供。

安全模块通过安全模块接口与中间件连接，中间件赋予每个模块一个“身份”号，每种安全模块接口允许挂接多个安全模块，一个安全设备也可以提供多种安全模块接口。

中间件支持动态加载安全模块，因此，每种应用可以同时向不同用户提供不同种类和级别的安全服务。

策略的修订或是提升安全服务质量可以通过简单的更换安全模块来完成，实现“即插即用”的功能。

这些模块可以直接提供给应用接口适配层，提供专业化的安全服务，是构建安全保障体系的主要平台。

2. 核心层

核心层主要提供各个模块之间的协调、保证自身的完整性、提供接入模块的认证管理。核心层实现了中间件的主要功能，是各个层次及其各个模块协同工作，并且提供可信的计算平台，抵御针对中间件的攻击，同时具有可扩展特性。该层包括：

（1）调度模块：调度模块负责协调不同安全模块、应用程序的调度及其接口管理。

（2）防护模块：利用模块认证与完整性检验，来保证自身的合法性与完整性，这是保证中间件作为可信计算平台的重要手段。

（3）功能扩展管理模块：每个层次允许增加新的模块，同时，还要加入新的接口交互语法目录，增加模块后的中间件要重新对其自身计算新的摘要和签名。

3. 协议适配层

协议适配层捆绑各种通用的及专有的安全协议，开发者无须再实现这些协议。目前，安全中间件的协议适配层通常能够支持 IPSec、SHTTP、TLS1.0/SSL3.0、S/MIME、WSS(XML/SOAP)等协议。开发者调用这些接口时仅需要将要处理的数据指向相应入口。另外，这些协议并不是集成在一起，而是相互独立的模块，开发之前需要选定一个或多个协议。如果不选择协议，用户可以直接使用基本的安全模块提供的功能。

4. 应用接口适配层

应用接口适配层为上层或应用程序提供各种类型的调用，涉及不同的开发平台与操作系统，通常提供标准 Java、C、C++、C# 等语言接口；同时还要提供接口数据格式的转换，如 ASCII、比特流、字符、国标字符等格式之间的转换。它为上层提供基本的安全服务接口 API，包括：认证服务、授权服务、密钥管理、密码服务、审计服务、安全管理等 API。

应用适配接口既可以直接提供给开发人员使用，也可以向应用中间件层提供接口。

3.8.3 分类

一般地，安全中间件分四类，即安全服务中间件、安全传输中间件、安全消息中间件和安全 Web 服务中间件。

1. 安全服务中间件

基本安全服务中间件为应用系统开发商提供专业化的安全服务接口，包括：认证服务、授权服务、密钥管理、密码服务、审计服务、安全管理等 API。它通常具有以下类型的接口：

(1) 认证服务接口：配合其他模块共同提供公钥证书生成、签发、注册、验证服务，负责证书库的维护和证书撤销列表的管理，以及信任模型的建立和可信时间戳服务，同时也包括传统的对称密钥认证服务。

(2) 授权服务接口：提供针对资源的授权管理和访问控制服务，包括基于 PMI 的授权服务以及传统的对称密钥授权服务；提供基于 LDAP 数据库存储策略库、属性库的访问接口。

(3) 密码服务接口：提供各种基本的密码运算，包括加解密、数字签名、完整性验证运算等；主要直接面向其他模块提供密码服务，也可以对应用程序提供专业化的密码服务。

(4) 密钥管理接口：提供密钥的产生、存储、备份、下发、归档、销毁等功能的接口，以及密钥管理策略的选择；主要直接面向其他模块提供密钥管理服务。

(5) 审计服务接口：提供审计信息的输入、分析结果的输出、审计数据库的管理接口、审计策略的设置接口等。

(6) 安全管理接口：为其他安全模块提供统一的安全管理接口。

2 安全传输中间件

安全传输中间件是在基本安全服务中间件的基础上，捆绑安全传输协议，提供安全的传输通道保护，可以应用于 IP、Socket、IIOP、FTP、TELNET 等协议的保护，用于应用网关、VPN 等设备。

这些捆绑的安全协议主要有：IPSec、TLS。另外还提供对其他一些安全传输协议的支持及用户订制协议的加载。

主要应用在 VPN 及加密防火墙等嵌入式系统、应用网关或代理服务器、安全电子邮件、原有的基于文件交换的消息中间件。提供安全的信息或文件传输通道。

3 安全消息中间件

安全消息中间件用于应用程序之间的信息交互，有多种形式，其中传输消息应用最广的格式有以下几类：XML 文件、SMTP/MIME 邮件消息等。

(1) 基于 XML 及 XML 文件的安全消息中间件利用标准的 SOAP 实现安全服务函数的远程调用，提供符合国际标准的安全协议或者提供定制的专有协议，由于其具有良好的互操作性及可扩展能力，具有广泛的应用前景。

(2) 基于 SMTP/MIME 邮件传输的安全消息中间件采用标准的 S/MIME 安全协议，属于存储转发类型的消息中间件。

(3) 基于 JMS 消息传送的安全中间件，广泛使用于 J2EE 平台。

安全消息中间件为各类应用程序消息传递(消息、邮件、文件)提供端到端细粒度的安

全保护。

4. 安全 Web 服务中间件

安全 Web 服务中间件主要用于同一应用系统内部或不同应用系统之间的安全交换及安全 Web 服务。它融合了 J2EE、CORBA、.NET 以及 Web 服务等主流分布式平台技术，支持 ebXML(电子商务 XML 可能会用于 G2B)、XML、SOAP 或是 Web 服务。提供细粒度、多层次安全保障的信息交换平台：传输层安全、应用层端到端安全。

3.9　无线网络安全技术

3.9.1　无线网络的特点

几年前，无线网络对于许多普通的网络用户而言，还是一个可望而不可即的梦。随着手机、无线网卡等简单无线设备的日渐普及，大家才真正体验到无线技术的无限魅力，以至于到现在，许多追求时尚和便捷生活的年轻人，已经对陪伴多年的有线鼠标也不习惯了，取而代之的是更为灵巧的无线鼠标。蓝牙耳机的逐渐兴起，随处可见的无线上网笔记本计算机，似乎都在告诉我们，我们的生活恐怕已经很难离开无线技术了。

但是，无线应用的便捷掩饰不了它与生俱来的局限性。与传统的有线网络相比，无线网络的安全性首先就是一个引人关注的问题。另外，同有线设备相比，无线设备具有 CPU 处理速度较慢、内存容量较小、通信链路带宽较小、输入法有限或完全不同、显示屏较小、电池寿命短等局限性，而且这些设备的网络访问方式也相对有限。从设备的物理安全角度来看，这些便携设备面临着更多的物理安全风险，例如，容易被盗，使用环境的温度、湿度、抗电磁干扰等物理条件不一定符合要求等。而且，相对于这些风险，对这些无线设备可以采用的安全保护技术措施实在是非常有限。例如，对于笔记本计算机而言，现在使用笔记本计算机锁的人为数不少。可真有人相信这样就足够安全了吗？和手机一样，一旦被盗，要追查回来，谈何容易！

当然，我们并不能因为这些局限性就望而却步了。事实上，对无线技术进行改进的尝试也从没停止过。这些改进最集中地体现在两个方面，一是对无线网络标准的改进；二是对无线设备功能与性能的改进。前者是某些无线网络信息技术专业人员、专业研究机构，尤其是热衷于技术探索的技术团体(包括标准化组织)的兴趣所在，后者则主要是靠一些设备制造商的不断努力。

目前，全世界互联网用户早已超过 10 亿，移动终端的数量也已经接近 10 亿。这些数字表明：随着时代的推移与技术的进步，人类对移动性和信息的需求正在急速上升，越来

越多的人希望在移动的过程中高速接入互联网，获取急需的信息，尽快完成想做的事情。无线通信的安全性因此显得愈发重要，对无线网络的安全性要求很高的网络应用也是层出不穷，其中，最典型的应用有移动电子商务和无线电子邮件存取应用等。

电子商务是利用现在先进的电子技术从事各种商业活动的方式。随着移动通信技术和无线网络的发展，电子商务正向移动和无线连接领域发展，从而出现了移动电子商务（Mobile Business 或 M-Business），移动电子商务使用移动设备进行电子商务交易活动，移动电子商务的具体的优点有：

（1）移动交易不受时间和地点的限制。

（2）效率高，大大节省了客户的交易时间。

（3）移动终端的身份固定，能够向用户提供个性化的移动交易服务。

（4）可以提供与位置无关的交易服务。

在移动电子商务中的应用主要包括以下具体的实现环节：

（1）网上银行：用户可以用移动设备通过网上银行轻松实现电话费缴纳、商场购物、缴泊车费、自动售货机买饮料、公交车付费、投注彩票等手机支付服务。如果在网上银行系统中采用了 WPKI 和数字证书认证技术，不法分子即使窃取了卡号和密码，也无法在网上银行交易中实现诈骗。从世界范围看，数字证书技术已经被广泛地应用在国内外网上银行系统中，至今尚未发现一例由于数字证书被攻破而使网上银行诈骗得逞的案件。网上银行主要包括无线电子支付和无线电子转账。

（2）移动支付标准：移动支付问题是移动电子商务中的关键问题，目前的移动支付标准主要有远程移动钱包标准和移动电子交易标准。

（3）移动设备安全：移动设备的安全主要是指移动设备本身的安全，包括操作环境的安全、密码和机密文件的安全，以及验证码和激活码的安全等。

此外无线网络安全问题也被用于无线支付方式的选项和 B2B 中，主要实现交易和支付的安全性。

由于商业活动信息交换的比较频繁而且实时性较强，商业人士可能会随时用电子邮件交换一些秘密的或是有商业价值的信息，因而用手机无线上网收发电子邮件就成为一种易用、高效的信息交换工具，这同时引出了一些安全方面的问题，例如，消息和附件可以在不为通信双方所知的情况下被读取、篡改或截掉，同时，发信者的身份也会被人伪造，可能造成不可挽回的经济损失。

在遵从可以发送加密和有签名邮件的安全电子邮件协议的前提下，采用 WPKI 技术可以解决这一问题。当用手机无线上网发送电子邮件给一位或多位接收人时，发送者可以先将邮件加密、签名。这样，只有指定的接收人才可以在 CA 中心的服务器上取得公钥并开启邮件，即使该邮件被其他人截获，这些人也会因为得不到公钥而无法阅读邮件。另

外，如果从采用的主要无线设备的角度进行分类，目前无线网络的主要应用有四种方式：移动电话、近地/中地轨道卫星电话网、无线 LAN 和无线电话(见图 3-9-1)。

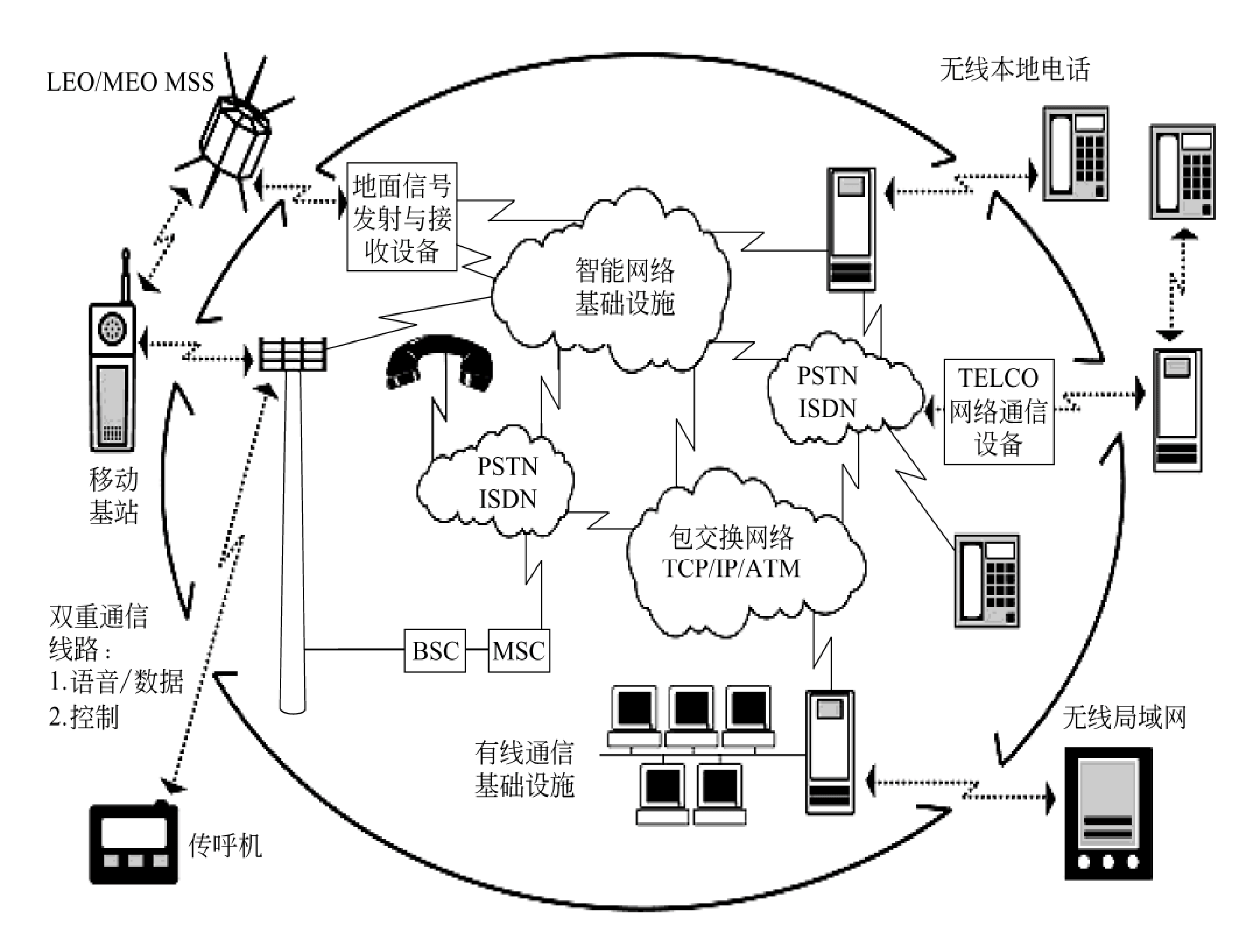


图 3-9-1　无线网络的主要应用示意图

这四种应用的功能要求、对网络环境的要求、互操作性要求不同，面临的威胁与可以采用的对策也彼此不同。

3.9.2　主要标准

1. 无线应用协议

无线应用协议(Wireless Application Protocol，WAP)的出现掀起了因特网发展的一次新的浪潮。WAP 是有线网络和移动通信网络的桥梁，大量的无线终端(如手机、PDA 等)通过 WAP 可以获取因特网上的大量的信息资源。但是同时，WAP 的安全性问题也得到人们的广泛的关注，由于在无线网路中，无线终端的数据处理能力有限，无线网络的带宽窄，时延长，稳定性差，这些原因导致了传统的有线网络安全问题不能在无线网络中得到应用。WAP 的安全体系结构有着区别于有线网络安全的特殊性。

WAP 是由 WAP 论坛制定,主要实现移动 Internet 接入的基本规程。WAP 的一系列通信协议将使新一代移动通信设备可靠的接入 Internet。如图 3-9-2 所示,WAP 的结构与万维网(WWW)结构有多类似的地方,最大的不同就在于在 WAP 的模型中增加了 WAP 网关;移动终端是通过 WAP 网关连接到有线网络中的服务器上的。

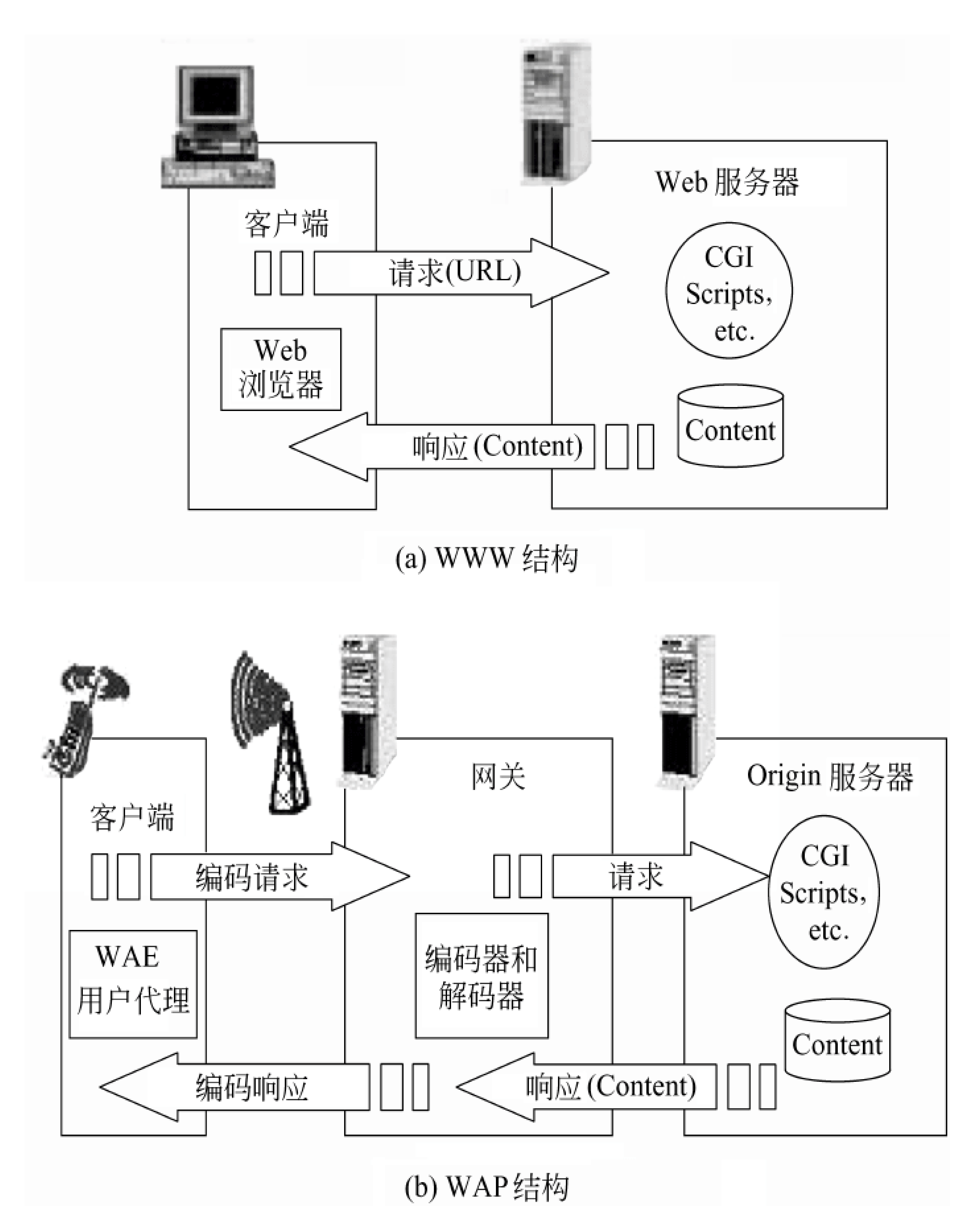


图 3-9-2　WWW 结构与 WAP 结构的比较

WAP 是由一系列的协议组成,用来标准化移动通信设备的网络访问服务。WAP 为移动通信应用开发提供了可伸缩的可扩展的环境,这种优越性建立在协议分层设计的基础上,结构中的每一层协议都可以被上层的协议访问,这种结构叫做"WAP 协议栈"。WAP 协议栈的设计参照了 WWW 的协议栈的设计,但是对 WWW 协议栈的传输的效率进行了优化,使得 WAP 更见适应于移动通信网络。

图 3-9-3 描述了 WAP 的协议栈,并且给出了 WAP 协议栈和有线网络协议栈的对比。从图中我们可以知道,WAP 主要分为无线应用环境(WAE)、无线会话协议(WSP)、

无线事务协议(WTP)、无线传输层安全(WTLS)、无线数据报协议(WDP)。

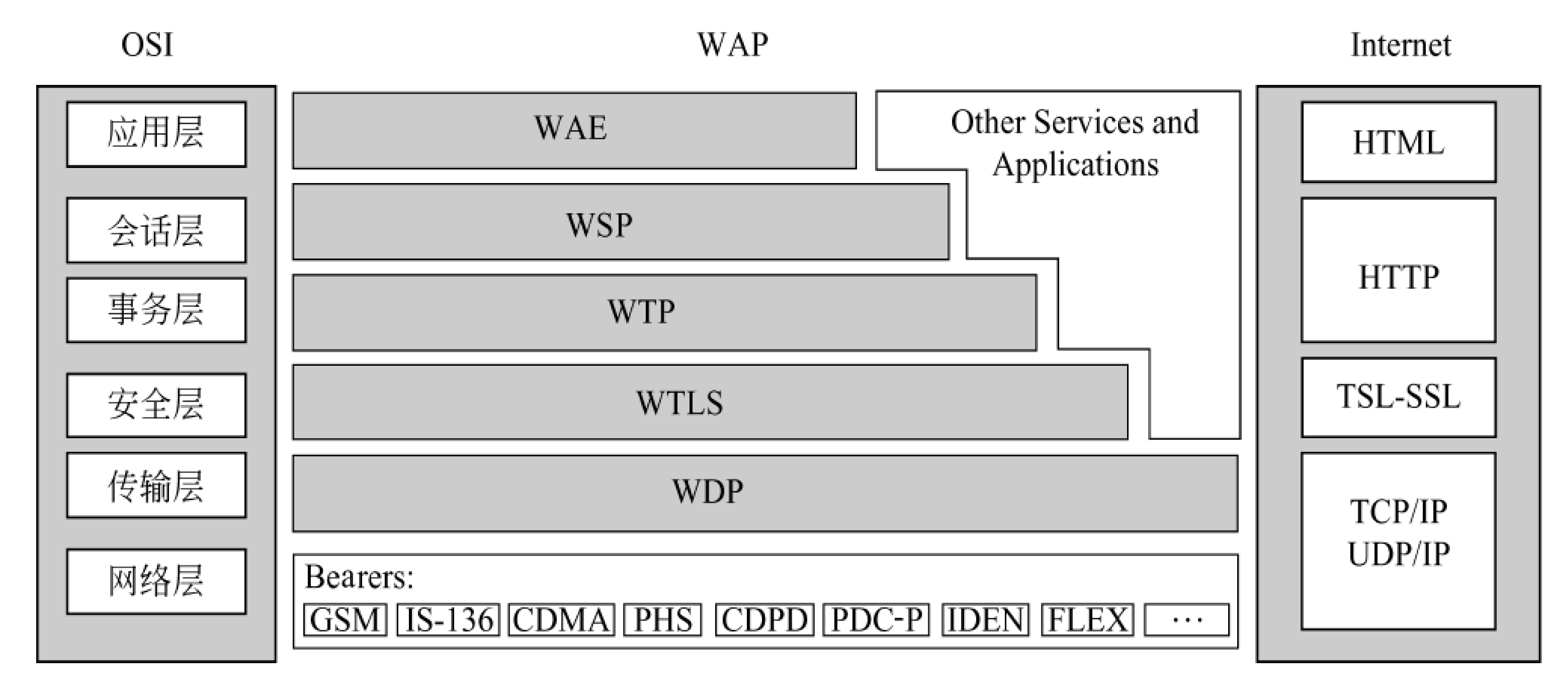


图 3-9-3　WAP 协议栈

WAP 的安全结构由 WTLS、WIM、WPKI、WMLScript 四部分组成,每个部分在实现无线网络安全中起着不同的作用。基于 WAP 的安全结构组成如图 3-9-4 所示。

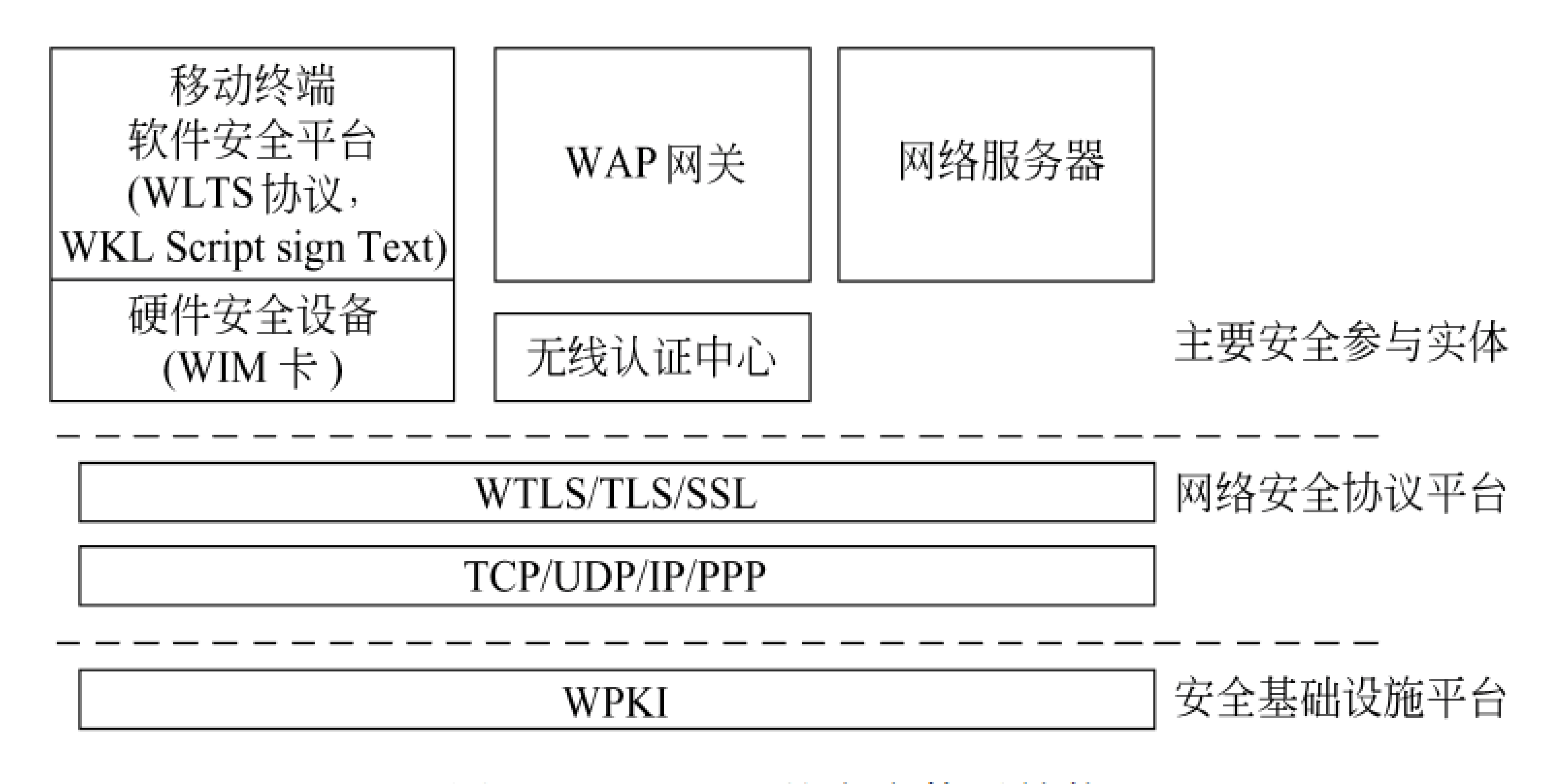


图 3-9-4　WAP 的安全体系结构

在该安全结构中,各主要组成部分的作用是:

1) 无线传输层安全(WTLS)

安全套接层(SSL)协议管理有线网络的在线通信,近年来,传输层安全(TSL)协议正在替代 SSL 成为 Internet 的安全协议,然后 WAP 的 WTLS 将 TLS 扩展到移动环境。WTLS 的主要目的是提供机密性,数据完整性和身份认证。在 WAP 结构中,TLS 或是 SSL 是在网络服务器和 WAP 网关之间使用;WAP 网关将 TLS 和 SSL 信息转换成 WTLS 信息,使得在无线网络中的数据传输更加的有效。WTLS 由功能协议层和记录协议层构成,其中功能协议层包括握手协议、改变密码规范协议、告警协议;记录协议层提供

对握手协议层以及上层应用数据的封装结构，在客户端和服务器端的 WTLS 对等层之间完成实际的数据传输任务。WTLS 协议的结构如图 3-9-5 所示。

握手协议	改变密码规范协议	告警协议
记录协议层		

图 3-9-5　WTLS 协议的结构

2）无线身份识别模块（WIM）

无线身份识别模块 WIM 是 WAP 定义的一个防篡改的硬件，它被用来执行安全层和应用层的安全功能，以及保存和处理用户 ID 和权限的功能。一般情况下，WIM 都是通过智能卡的形式实现的，比如单独的 WIM 卡，或是和 SIM 卡结合，形成 S/WIM 卡。WIM 解决安全方面的两个基本的问题：第一是在 WAP 网关和移动终端之间实现 WTLS 协议，WIM 通过保存在智能卡中的密码算法来执行通信双方的验证和校验的功能；第二是通过数字签名和非否认技术来保证应用层的安全。

3）无线 PKI（WPKI）

无线 PKI 是由 WAP 论坛提出的一个标准，主要在 WAP 的安全结构中负责证书的发放，管理以及相关的操作。WPKI 对 PKI 做了一些必要的改动，使之更加适合无线网络环境。WPKI 采用非对称密码算法和原理来提供移动通信网络中的安全服务，包括身份认证，数据完整性和加密等服务。在具体的实施上，WPKI 采用证书作为密钥对的管理手段，可以说，WPKI 是 WA 安全的基础。图 3-9-6 描述了 WPKI 的结构和工作流程。

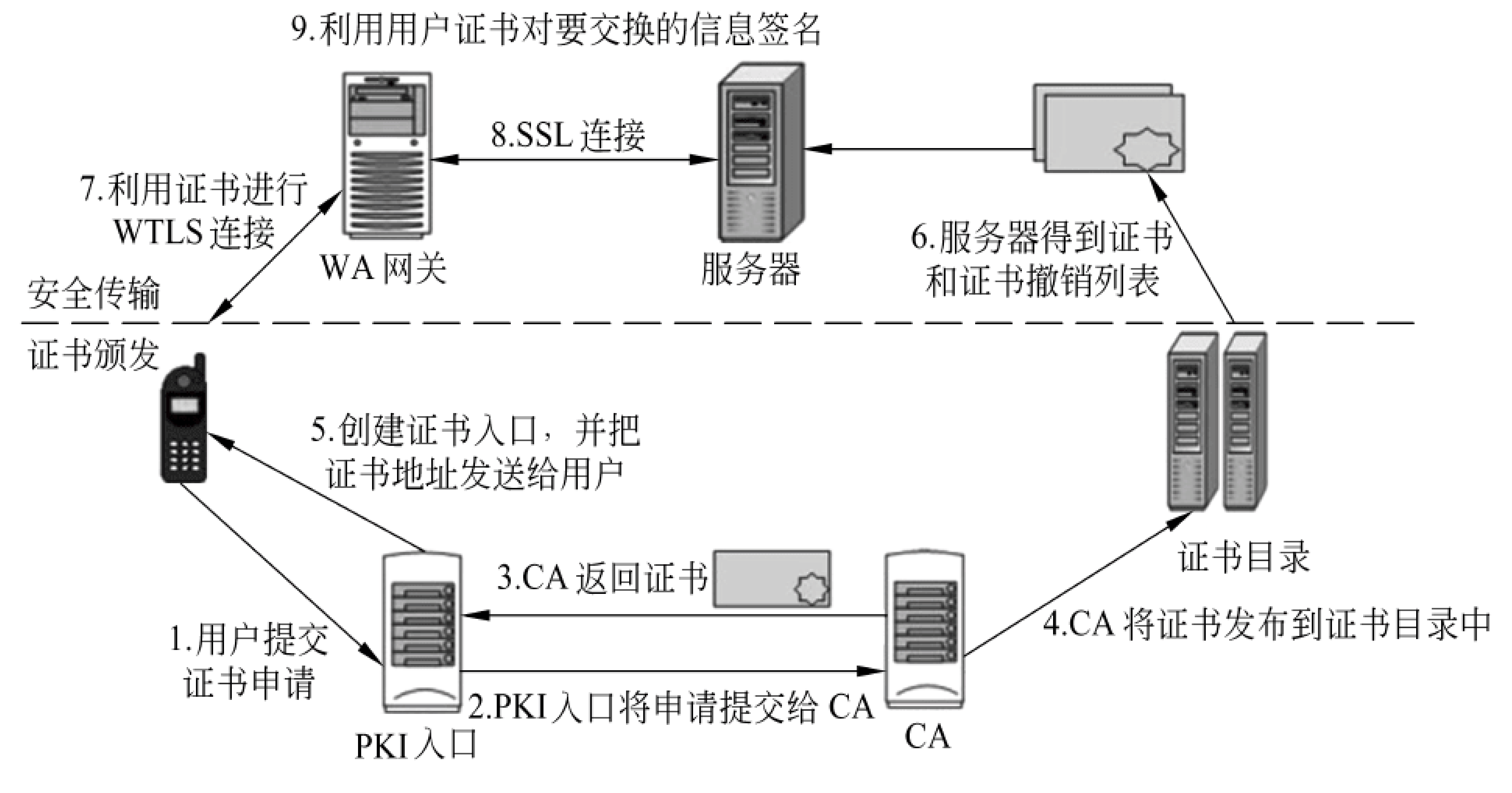


图 3-9-6　WPKI 的结构和工作流程

WPKI 中定义了三种不同的安全通信模式：

（1）使用服务器证书的 WTLS Class 2 模式：这种模式中，客户端可以验证它连接的服务器的身份。

(2) 使用客户端证书的 WTLS Class 3 模式：这种模式中，服务器验证了请求连接的客户端的身份。

(3) 使用客户端证书合并 WTLS Script 的 signText 模式：signText 模式中，基本的功能和 Class3 的功能很是类似，但是主要的区别是 WTLS Class 3 模式也支持移动终端与网关的安全连接和移动终端与网络服务器的安全连接两种情形。

目前，WPKI 已经能够支持 X. 509 v3、X9. 68、WTLS 格式的证书。依据 WAP-199-WTLS 规范中的定义，证书内容应该包括：

(1) Certification version：值为 51。

(2) Signature algorithm：用于签署证书的算法。

(3) Issuer：Client 端信任的一家证书颁发机构。

(4) Valid not before：证书有效期开始，UNIX32 位格式。

(5) Valid not after：证书有效期终止，UNIX32 位格式。

(6) Subject：公钥所有者。

(7) Public key type：公钥算法。

(8) Parameter specifier：任何与公钥相关的参数。

(9) Public key：公钥。

4) WMLScript

WMLScript 是运行在手机上的脚本程序，和 JAVAScript 很有类似之处，不同之处就在于 WMLScript 必须放在一个 WMLS 文件中，并且 WMLS 文件的大小不能大于 1. 4KB。

WMLScript 给应用程序提供了以下功能：

(1) 在发往网络服务器之前对用户输入进行了有效地检查。

(2) 访问设备的设施和外围。

(3) 同用户交互而不引发到服务器的往返(例如：显示错误信息)。

事实上，在 WMLScript 中，实现安全功能的主要是 signText 函数。signText 函数主要实现客户端消息的签名，然后把签名和消息一起发送出去，由服务器端验证签名。

2. 802.11 无线局域网标准

无线局域网(Wireless Local Area Network，WLAN)采用相应的标准，实现对现有有线 LAN 的扩展，使用无线电波承载数据，使数据在短距离中以高传输率被传送到装备了无线电接收器和发送器的设备中。

目前使用最多的无线局域网标准是 802. 11a/b/g。802. 11 规范了无线局域网的介质

访问控制层(MAC)和物理层,使得各个不同的厂商的产品可以互连。图 3-9-7 描述了完整的 802.11 的协议实体。

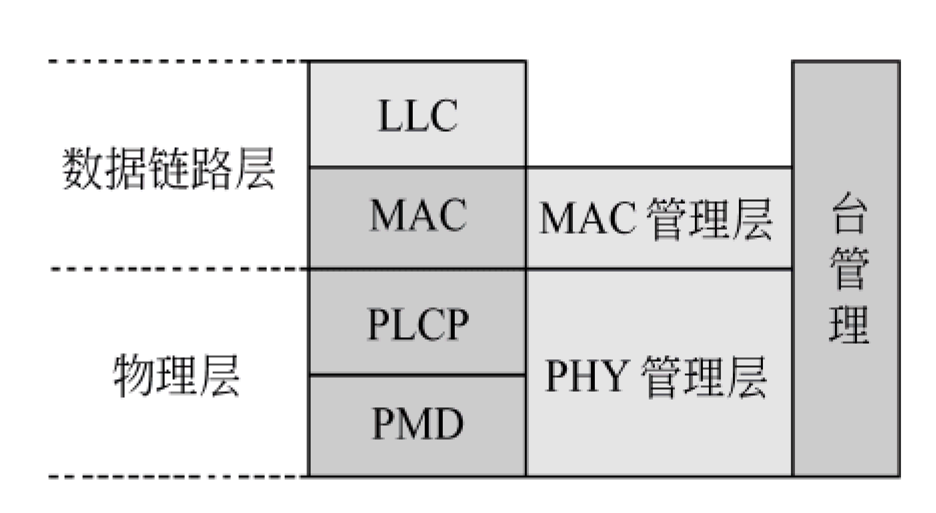


图 3-9-7　802.11 的协议实体

其中,MAC 层分为 MAC 子层和 MAC 管理子层。MAC 子层主要负责访问控制的实现和分组的拆分和重组。MAC 管理子层主要负责 ESS 漫游管理,电源管理,还有登记过程中的关联,去关联以及要求重新关联等过程的管理。

802.11 的物理层分了三个子层:物理层会聚协议(PLCP),物理介质相关协议(PMD)和物理层管理子层。PLCP 子层主要进行载波侦听的分析和针对不同的物理层形成相应的分组。PMD 子层用于识别相应的介质传输信号所使用的调制和编码技术。物理管理子层为不同的物理层进行信道选择和协调。

除此之外,IEEE 802.11 还定义了一个台管理子层,主要任务是协调物理层和 MAC 层之间的交互作用。

在 802.11a/b/g 中,802.11b 应用最为广泛。该协议有两个主要组件,即远程设备中的无线网络接口卡(NIC)和无线接入点(Access Point)。802.11b 标准为其分配了 11 个信道。流量可以进一步通过使用扩展服务区 ID(ESSID)进行分段。ESSID 是接入点与无线 LAN 适配器之间一个共享的、明文方式的名称。如果 LAN 适配器与接入点的 ESSID 相同,就允许 LAN 适配器与接入点相连。

3.9.3 无线局域网

无线局域网(Wireless LAN,WLAN)的技术和产业可以追溯到 20 世纪 80 年代中期,美国联邦通信委员会(FCC)使用了扩频技术,在随后的几年中发展的很慢,但是由于 802.11b 标准的制定,现在 WLAN 技术发展的很快。无线技术在便利性和成本上的两个优势,使得它无需布线,灵活方便,且产品已经很多很成熟,范围一般在室内 100m,室外 300m 左右,所以不需要把使用者束缚在他们的桌子上,就可以得到需要的数字资源。

WLAN 技术的优势主要体现在核心业务优势和运营优势两方面。核心业务优势包括提高了雇员的工作效率、提高了业务进程的速度和效率以及增大了创建全新业务功能的可能性。运营优势包括降低管理成本和降低资本支出。

其中,WLAN 的核心业务优势主要在于提高了员工工作的灵活性和机动性,例如:

(1) 通过建立与企业局域网 (LAN) 的透明连接,在办公室与办公室间活动的人、进入办公室的远程工作人员都节省了不少时间,避免了很多麻烦。无线网络覆盖的任何物理位置都可即时建立可用连接,而无需寻找网络端口、电缆或 IT 人员来帮助您连接到网络。

(2) 无论知识顾问位于建筑物的任何位置,需要其帮助的员工都可与之保持联系。通过电子邮件、电子日历和网络聊天,员工无论在开会还是离开办公室,都可保持联机状态。

(3) 联机信息随时可用。如果会议中有人急需检索上个月的图形报告或更新演示文稿,无需中断会议。这将极大提高会议的质量和效率。

(4) 提高了组织的灵活性。随着团队和项目结构的更改,快速、轻松地移动办公桌,甚至移动整个办公室都会成为可能,员工不会再受到办公位置的束缚。

WLAN 技术的主要运营优势是具有较低的资金和运营成本,这可以具体归纳为三点:

(1) 建筑物联网的成本大幅度降低。尽管多数办公室空间都铺设了网络电缆,但仍有许多其他工作场所(例如,工厂、仓库和商店)尚未铺设。无线网络还可以在无法建立有线网络的位置(例如,户外、海上甚至战场)提供。

(2) 可以根据组织需求来调整网络(如果需要,甚至可以每天调整),使之满足不同层次的需求;在给定位置部署高度集中的无线接入点 (AP) 要比增加有线网络的端口数容易得多。

(3) 构建基础结构再也不需要考虑资金,可以轻松地将无线网络基础结构移动到新的建筑物,而有线网络永远是固定的。

虽然 WLAN 具有上述优势,但与其相关的许多安全问题还是限制了这项技术的使用。金融和政府等比较关注 WLAN 安全的行业部门,尤其担心通过 WLAN 将没有得到足够保护的数据传播给周围地区的人,非常危险。目前,大多数业务已经实施了某种形式的无线安全性,但这种安全性通常只是采用了最为基本的第一代无线安全功能。而按照现今的需求标准来考虑,它所提供的保护措施是远远不够的。

一般地,WLAN 应用主要存在以下几种不安全因素:

(1) 窃听(数据泄漏)。窃听网络传输数据可导致机密数据泄漏、未保护的用户凭据泄漏,以及身份被盗用。还使得有经验的入侵者能够收集用户的 IT 环境相关信息,然后利用这些信息攻击其他情况下不易遭到攻击的系统或数据。

(2) 截获和修改传输数据。如果攻击者可以访问网络,他(或她)便可插入恶意计算机来截获和修改两个合法方之间交换的网络数据。

(3) 哄骗。如果可以访问内部网络,入侵者便可以采用一些在网络外部无效地方法伪造表面上合法的数据,例如,一封哄骗性的电子邮件。相比之下,员工(包括系统管理员)通常更容易相信来自企业网络内部的信息,而不是来自网络外的信息。

(4) 拒绝服务(DoS)。一个攻击者可能会以各种方式触发 DoS 攻击。例如,攻击者会通过简单的技术(如微波炉)触发无线电级信号干扰。复杂的攻击多是针对低层无线协

议本身;不很复杂的攻击则通过向 WLAN 发送大量的随机流量而使网络堵塞。

(5) 免费下载(或资源盗用)。入侵者最邪恶的举动是利用被攻击者的网络作为自己访问 Internet 的自由访问点。这虽不像其他威胁那么有杀伤力,但至少不仅会降低合法用户的服务可用级别,还可能会引入病毒和其他安全威胁。

(6) 偶然威胁。某些 WLAN 功能可使无意的威胁引发祸端。例如,合法访问者可能在启动便携式计算机时无意间连接了用户的网络,然后自动连接到用户所在的 WLAN。现在,访问者的便携式计算机是病毒侵入网络的潜在入口点。这种安全威胁是 WLAN 应用中存在的一个最为明显的安全问题。

(7) 恶意 WLAN。即便某些公司尚未正式启用 WLAN,仍会受到在公司的网络上出现的非法托管 WLAN 的威胁。热心的雇员购买的低价位 WLAN 硬件会使这些公司的网络出现意外的安全漏洞。

早期的无线网络标准安全性并不完善,技术上存在一些安全漏洞。但是,由于 WLAN 标准是公开的,随着使用的推广,更多的专家参与了无线标准的制定,使其安全技术迅速成熟起来。现在不只是在家庭,学校,中小企业里边 WLAN 得到广泛的应用,在对于信息安全需求更为敏感的大企业、金融机构、政府机构,WLAN 的安全性与可靠性也得到了进一步认可,并得以大量地推广使用。

为了有效保障无线局域网的安全性,必须实现三个基本的安全目标,分别是:

(1) 提供接入控制:验证用户,授权他们接入特定的资源,同时拒绝为未经授权的用户提供接入。

(2) 确保连接的保密与完好:利用强有力的加密和校验技术,防止未经授权的用户窃听、插入或修改通过无线网络传输的数据。

(3) 防止 DoS 攻击:确保不会有用户占用某个接入点的所有可用带宽,从而影响其他用户的正常接入。

事实上,当前无线局域网安全技术的快速发展和应用,已经为无线网络的安全提供了一定程度的保障。这些保障性的技术措施主要有以下六种:

1) 服务区标识符匹配

服务区标识符(Service Set Identifier,SSID)将一个无线局域网分为几个不同的子网络,每一个子网络都有其对应的身份标识 SSID,只有无线终端设置了配对的 SSID 才接入相应的子网络。所以可以认为 SSID 是一个简单的口令,提供了口令认证机制,实现了一定的安全性。但是这种口令极易被无线终端探测出来,企业级无线应用绝不能只依赖这种技术做安全保障,而只能作为区分不同无线服务区的标识。

2) 无线网卡物理地址过滤

每个无线工作站网卡都由唯一的物理地址(MAC)标识,该物理地址编码方式类似于

以太网物理地址，是 48 位。网络管理员可在无线局域网访问点 AP 中手工维护一组(不)允许通过 AP 访问网络地址列表，以实现基于物理地址的访问过滤。其优点是：简化了访问控制、接受或拒绝预先设定的用户、被过滤的 MAC 不能进行访问、提供了第二层的防护。缺点是：当 AP 和无线终端数量较多时，大大增加了管理负担、容易受到 MAC 地址伪装攻击。

3）有线等效保密

IEEE 80211.b 标准规定了一种被称为有线等效保密(Wired Equivalent Privacy，WEP)的可选加密方案，其目的是为 WLAN 提供与有线网络相同级别的安全保护。WEP 采用了静态的有线等同保密密钥的基本安全方式。静态 WEP 密钥是一种在会话过程中不发生变化也不针对各个用户而变化的密钥。WEP 在传输上提供了一定的安全性和机密性，能够阻止有意或无意的无线用户查看到在 AP 和 STA 之间传输的内容。静态 WEP 密钥的优点在于：全部报文都使用校验和加密，提供了一些抵抗篡改的能力、通过加密来维护一定的机密性，如果没有密钥，就难把报文解密、WEP 非常容易实现、WEP 为 WLAN 应用程序提供了非常基本的保护。同时，静态 WEP 密钥的局限性也很明显，主要是它对于 WLAN 上的所有用户都是通用的，缺少密钥管理，ICV 算法不合适，RC4 算法存在弱点，以及认证信息易于伪造。

4）端口访问控制技术(IEEE 802.1x)和可扩展认证协议(EAP)

尽管 802.1x 标准最初是为有线以太网设计制定的，但它也适用于符合 802.11 标准的无线局域网，并且被视为是 WLAN 的一种增强性网络安全解决方案。802.1x 体系结构包括三个主要的组件：

(1) 请求方(supplicant)：提出认证申请的用户接入设备，在无线网络中，通常指待接入网络的无线客户机 STA。

(2) 认证方(authenticator)：允许客户机进行网络访问的实体，在无线网络中，通常指访问接入点 AP。

(3) 认证服务器(authentication sever)：为认证方提供认证服务的实体。认证服务器对请求方进行验证，然后告知认证方该请求者是否为授权用户。认证服务器可以是某个单独的服务器实体，也可以不是。如果它不是单独的服务器实体，通常是已经将其认证功能集成在了认证方认证服务器中。

802.1x 认证一般包括以下六种 EAP(Extensible Authentication Protocol)认证模式：EAP-MD5、EAP-TLS(Transport Layer Security)、EAP-TTLS(Tunnelled Transport Layer Security)、EAP-PEAP(Protected EAP)、EAP-LEAP(Lightweight EAP)、EAP-SIM。

802.1x 认证的优点主要体现在四个方面：

(1) 802.1x 协议仅仅关注受控端口的打开与关闭。

(2) 接入认证通过之后,IP 数据包在二层普通 MAC 帧上传送。

(3) 由于是采用 Radius 协议进行认证,可以很方便地与其他认证平台进行对接。

(4) 提供基于用户的计费系统。

但是,它的缺点也很明显。首先,它只提供用户接入认证机制,没有提供认证成功之后的数据加密,用户的数据仍然是使用的 RC4 进行加密。其次,它一般只提供单向认证。此外,它提供的是 STA 与 RADIUS 服务器之间的认证,而不是与 AP 之间的认证。

5) WPA (Wi-Fi 保护访问) 技术

市场对于提高 WLAN 安全的需求是十分紧迫的。IEEE 802.11i 的进展并不能满足这一需要。在这种情况下,Wi-Fi 联盟制定了 WPA(Wi-Fi Protected Access)标准。WPA 是 IEEE 802.11i 的一个子集,其核心就是 IEEE 802.1x 和 TKIP。

尽管 WPA 在安全性方面相比 WEP 有了很大的改善和加强, 但 WPA 只是一个临时的过渡性方案,在 WPA2(802.11i)中将会全面采用 AES 加密机制。

6) 高级的无线局域网安全标准——IEEE 802.11i

IEEE 802.11i 规定使用 802.1x 认证和密钥管理方式。在数据加密方面,定义了 TKIP(Temporal Key Integrity Protocol)、CCMP(Counter-Mode/CBC-MAC Protocol)和 WRAP(Wireless Robust Authenticated Protocol)三种加密机制。其中,TKIP 采用 WEP 机制里的 RC4 作为核心加密算法,可以通过在现有的设备上升级固件和驱动程序的方法达到提高 WLAN 安全的目的。CCMP 机制基于 AES(Advanced Encryption Standard)加密算法和 CCM(Counter-Mode/CBC-MAC)认证方式,使得 WLAN 的安全程度大大提高,是实现 RSN 的强制性要求。

对于 WLAN 系统,如果不从整体上进行规划和设计,只孤立地采用单一的某项安全技术,一般都无法满足用户高级别的安全性要求,反而会造成无线网络不安全的表象,导致用户不能充分利用无线网络所能提供的诸多特性和优点来进行资源共享和提高工作效率。因此,必须根据用户的实际情况和需求,综合运用多种安全技术。

那么,究竟应该如何将一个无线局域网设置成为安全的网络呢? 一般地,可以从以下四方面来考虑。

1) 选择恰当的物理位置和访问方式

对于安全性而言,接入点的位置非常关键,需要考虑它的可访问性和信号范围。接入点的位置应该放在攻击者很难修改或是窜改接入点设置的地方。此外,还要确保不能通过远程方式对接入点进行配置,尤其是不能通过无线的远程方式对接入点进行配置。

另一个问题来自于对信号强度的考虑。一定要对无线信号进行测量,确定接入点的位置,使得合法用户范围内的信号强度较强,合法用户范围之外的信号强度较弱。

2）进行接入点安全配置

构建无线安全网络的下一个步骤是配置接入点。每一种产品的出厂设置是基本相同的，因此在接入点接入网络之前修改默认配置非常重要。SSID 和接入点名称这些默认的配置一定要修改，同时要注意在 SSID 和名称中不要出现公司的名称、所在地，制造商名称等信息，还要关闭接入点的 SSID 广播，在这之后再启动 WEP 的 128 位的密钥模式。要定期修改 WEP 密钥，防止该密钥被攻破。至于很多接入点和网络所提供的动态主机配置协议（DHCP）功能。由于从安全的角度来看，这种服务对地址请求的控制非常有限，建议关闭该项服务。除此之外，还必须在接入点上进行 MAC 地址过滤确保只有那些被指定的在 MAC 地址表中的网卡才能访问无线局域网。

3）安全的网络设计方案

采用安全的网络设计方案，是实现无线局域网安全重要手段。这里，首先要考虑的就是无线接入点的放置问题，应该将它放置在不可信的网段，并采用一些措施将可信网段和不可信网段隔离开，这样就可以保护可信网络，即使是攻击者连接上了接入点，破解了 WEP 密码，他们也无法访问可信网络中的数据。

此外，也可以使用 VPN 技术实现网络安全连接。VPN 既可以对用户进行身份的验证，也可以提供密码服务。VPN 服务器的使用有两种方法：一种是使用单独的防火墙，另一种是使用更加安全的双重防火墙。

图 3-9-8 所示的无线局域网使用了一个单独的防火墙。

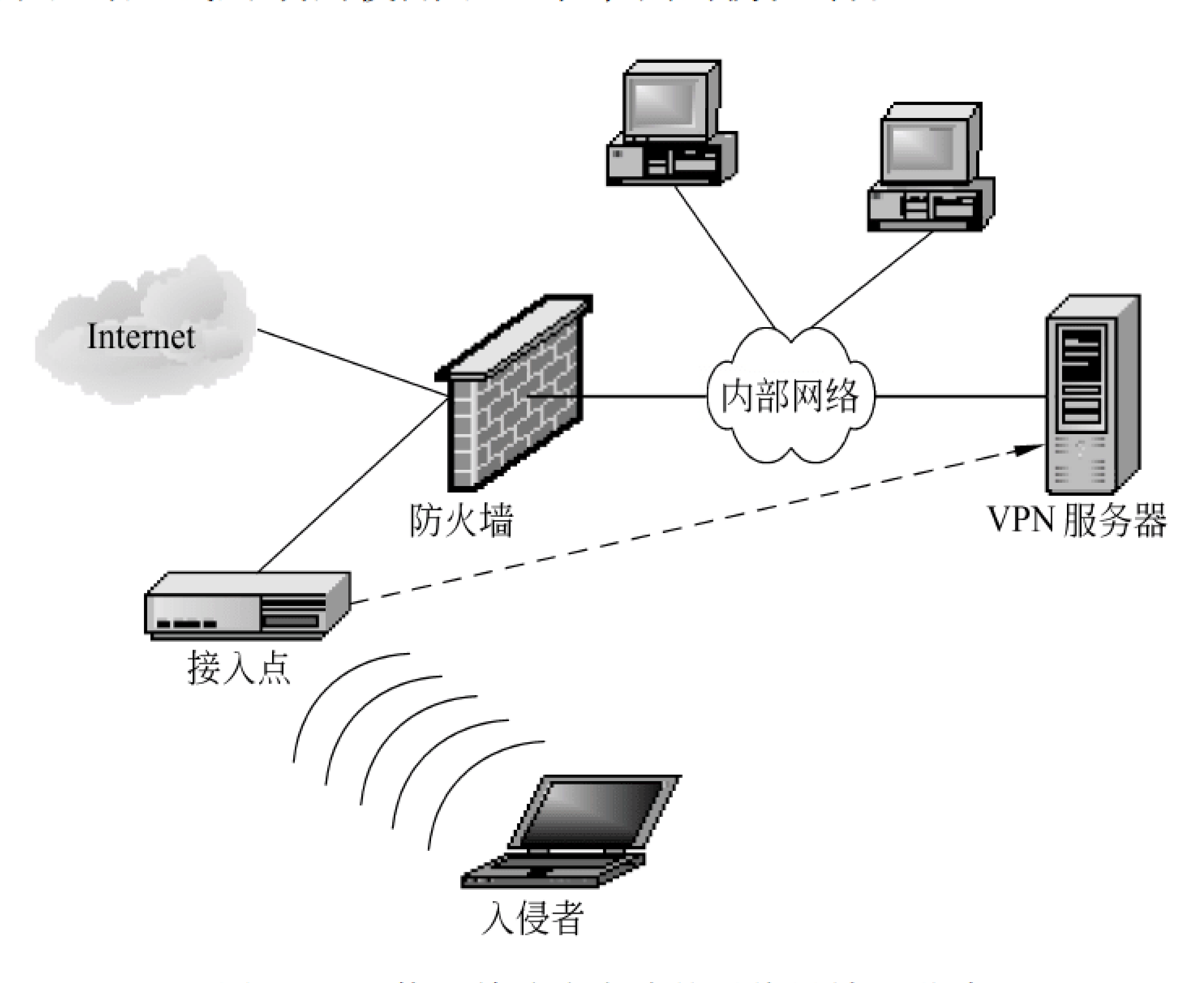


图 3-9-8　使用单独防火墙的无线局域网设计

使用的单独防火墙将内部网络和接入点隔离开,VPN 服务器包含在内部网络中。通常情况下,这种设计也不是最安全的,因为 VPN 服务器遭受的任何威胁都会导致内网的安全性下降。为了实现这种 VPN 的设置,需要在防火墙上安装另一层网络接口,使这个新的接口只能连接到接入点上,而且还要为这些接口编写一个单独的防火墙规则,允许无线网络到 VPN 服务器的通信,同时禁止该接口的其他任何通信。

单独防火墙解决方案能够满足认证和加密的要求,但不是很理想。因为内部网络的安全性完全依赖于 VPN 服务器的安全性。如果 VPN 服务器受到攻击,那么攻击者就可以攻击内部网络中的任何一个机器。

图 3-9-9 是一双重防火墙的解决方案。

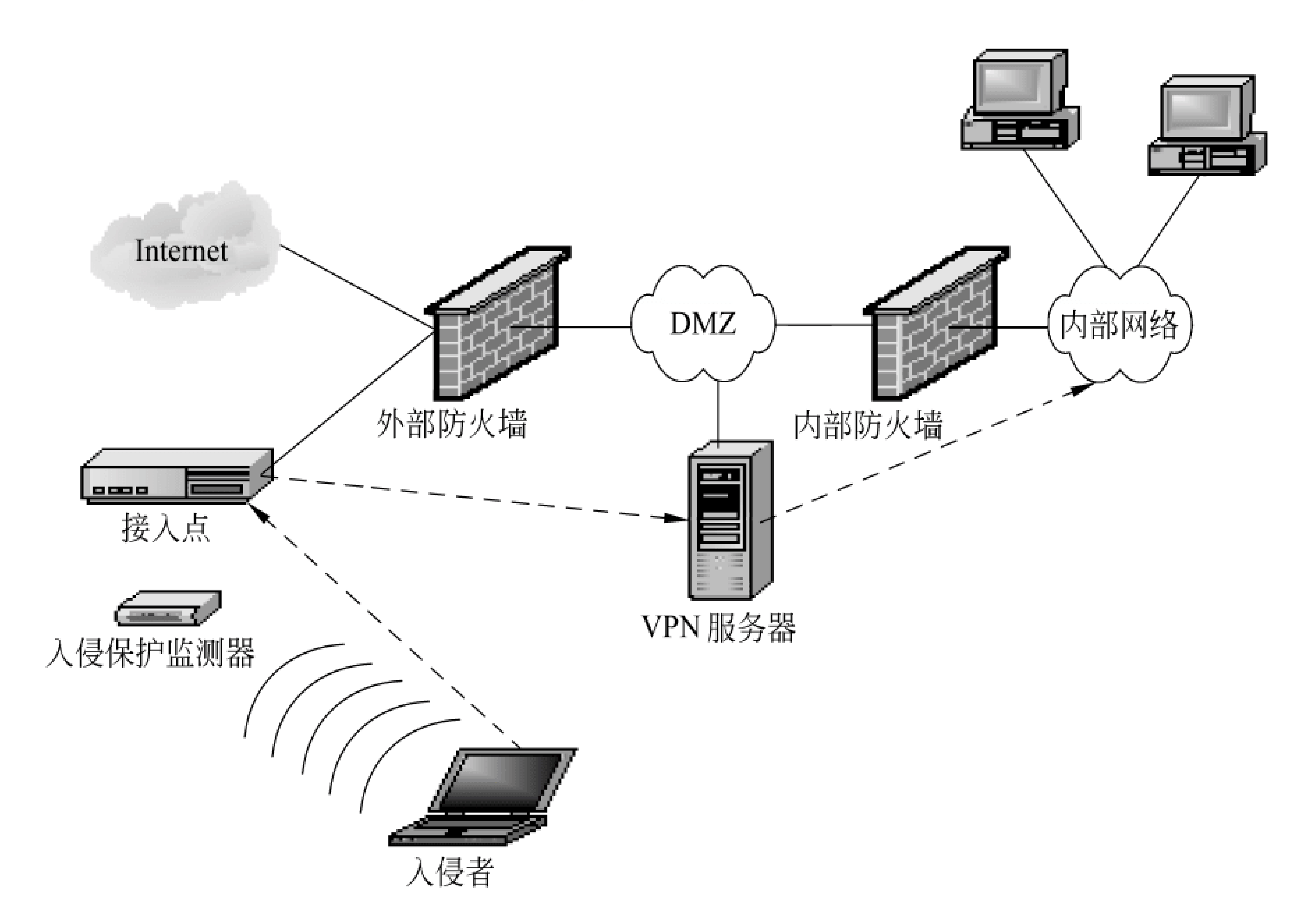


图 3-9-9　使用双重防火墙的无线局域网设计

该图中的两个防火墙,一个是保护内部网络的,一个是面向接入点的。两个防火墙之间是非军事区 DMZ(这是添加在受保护网络和外部网络之间的网络,可以将敏感的信息和公共信息隔离)在这种情况下,可以将 VPN 服务器放在 DMZ 中。只允许接入点同 DMZ 中的 VPN 服务器进行通信。这样,即使 VPN 服务器遭受威胁,并不能使攻击者攻击内部网络。

此外,也可以在上述网络中添加一个入侵检测系统(IDS)。IDS 的位置可以是在接入点所在的不可信网段,这样有助于提醒管理员可能发生的潜在威胁。

在这种设计中,除了设置 VPN,还可以直接将 WEP 升级为 WPA,或是直接采用

802.11i。但是通常都不建议放弃防火墙的设置。

4）通过策略进行保护

在启动无线网络之前，还应该制定网络的安全策略。安全策略是一个或一系列便于理解和及时修改的文档。安全策略必须规定不能在内网中放置规划之外的接入点，因为一旦有了非法的接入点，整个网络的安全性就大大降低了。

安全策略还应该详细描述更新用户工组站上的 WEP 密钥的方法及其操作过程。这种操作可以手动完成，也可以通过加密电子邮件的形式进行。

3.10 小结

本章介绍了密码服务、密钥管理、认证、授权、容灾备份与故障恢复、恶意代码防范、入侵检测、安全接口与中间件、无线网络安全九种信息安全技术的基本原理、主要作用、通用要求和体系结构。

鉴于这些技术都有各自丰富的内涵，我们在很多时候也称其中的每一个是一个单独的技术体系。但是，在实际应用中，我们很难找到仅仅采用了其中一种技术的网络与信息系统。原因很简单，任何一种单一的技术都无法满足我们的现实需要。如何在综合采用这些技术的基础上，权衡利弊，综合防范，是一个不断吸引众多学者和技术专家努力探讨的话题。

我们相信，随着新需求的出现和技术的进步，将会有某些技术彼此更为密切地融合，不分彼此，从而改变我们在这里所述的技术分类格局。同时，也会有某些技术逐渐淡出人们的关注视野。这正是我们不断探索研究的动力所在。

习　题

简答题：

1. 密码服务系统通常由哪些部件组成？这些部件各自的作用是什么？
2. 一个实际的应用系统会涉及哪些密码应用？
3. 密码服务系统接口的主要功能是什么？
4. 密钥管理基础设施主要有哪些功能？密钥管理系统的逻辑组成主要有哪些组件？
5. 请简要说明认证体系的组成及其核心组件 CA 的主要作用。
6. 什么是目录服务？什么是目录树？认证体系中的目录服务通常采用什么协议？
7. 请简要描述认证体系的三种基本信任模型。

8. 什么是交叉认证？什么是桥 CA？

9. 请简要说明可信时间戳的组成。

10. 生物特征识别可以采用的生物特征有哪些？

11. 简述授权体系的基本结构，并详述策略实施点和策略决策点的作用。

12. 请简要说明容灾备份与故障恢复系统的运作过程。

13. 制定具体的备份策略必须遵循哪些原则？建立异地备份中心需要满足什么基本要求？

14. 数据备份有几种主要类型？实现数据备份的方式有哪几种？

15. 进行系统恢复有哪些主要措施？进行数据恢复需要考虑哪些因素？

16. 网关防病毒系统的功能要求主要是什么？

17. 什么是入侵检测？CIDF 定义的五类入侵检测系统构件分别有什么作用？

18. 入侵检测系统有几种分类方法？基于行为的入侵检测的基本原理是什么？

19. 什么是中间件？它有什么特点？简要描述安全中间件的体系结构。

20. WAP 的结构与万维网(WWW)的结构有什么不同之处？

21. 简要说明 WAP 协议栈和有线网络协议栈的联系。

22. WAP 的安全体系结构中的 WPKI 具有什么结构？简要说明 WPKI 的工作流程。

23. 802.11b 协议的主要组件是什么？ESSID 有什么作用？

24. 保障 WLAN 的技术措施有哪些？

实践题：

25. 介绍你所了解的动态口令应用。

26. 浏览一些常见的电子商务网站，描述你所观察到的网上支付方式，分析其中可能存在的技术漏洞以及解决办法。

27. 对比工商银行、招商银行的网上银行业务模式，说明其各自的特点。

28. 描述你所使用过的一种 CA 的证书格式。

29. 选择一台恰当的可控目标主机，尝试一种网络入侵工具，说明它的主要特点和功能，记录你的操作步骤和操作结果。

30. 选择一个可控的 LAN，尝试一种网络扫描工具，说明它的主要特点和功能，记录你的操作步骤和操作结果。

31. 借助必要的软件工具，查找自己计算机上是否存在恶意代码，并手工清除。记录你的操作步骤和操作结果。

第 4 章 主要信息安全产品

目前市场上的信息安全产品种类很多，而且还在像雨后春笋一样不断涌现，我们不可能逐一介绍也没必要逐一介绍。本章主要介绍目前常见的 10 类信息安全产品，结合第 3 章所介绍的相关技术描述这些产品的主要功能、特点、局限性、发展趋势，并举例说明一些代表性产品的应用情况。

4.1 网络边界防护产品——入侵检测系统

目前国内外已有很多入侵检测系统(IDS)生产厂商和产品，国内主要的 IDS 生产厂商有金诺网安、启明星辰、绿盟科技等。事实上，3.7 节已经介绍了 IDS 产品的功能特点和分类，本节主要介绍 IDS 产品的局限性和发展趋势。

4.1.1 局限性

近 20 年来，由于网络攻击者的攻击水平不断提高，攻击工具与攻击手法日趋多样，以及以黑客为代表的攻击者不遗余力地与所有安全产品进行着斗争，IDS 等网络安全产品也不断更新换代，IDS 产品逐渐地从一个简单产品发展成为智能化的产品直至发展到入侵防御系统(IPS)产品。但是，这种发展似乎总落后于实际需求。

目前看来，IDS 还存在很多问题，有待于进一步完善。这些问题主要是：

1. 误警(误报)率高

误警的传统定义是将良性流量误认为恶性的。广义上讲，误警还包括对 IDS 用户不关心事件的告警。因此，导致 IDS 产品高误警率的原因是 IDS 检测精度过低以及用户对误警概念的拓展。

2 产品适应能力低

传统的 IDS 产品在开发时没有考虑特定网络环境的需求，千篇一律。网络技术在发展，网络设备变得复杂化、多样化，这就需要入侵检测产品能动态调整，以适应不同环境的需求。

3. 大型网络的管理存在缺陷

很多企业规模在不断扩大，对 IDS 产品的部署从单点发展到跨区域全球部署，这就将公司对产品管理的问题提上日程。首先，要确保新的产品体系结构能够支持数以百计的 IDS 传感器；其次，要能够处理传感器产生的告警事件；此外，还要解决攻击特征库的建立、配置以及更新问题。

4. 主动防御功能不足

目前市场上 IDS 产品的主动防御功能普遍不足，需要在下一代 IDS 产品中增强主动防御功能，以增强其主动性。

5. 处理速度上的瓶颈

随着高速网络技术如 ATM、吉比特以太网等的相继出现，如何实现高速网络下的实时入侵检测是急需解决的问题。目前的百兆、吉比特 IDS 产品的性能指标与实际要求还存在很大的差距。

6. 评价 IDS 产品没有统一标准

对 IDS 进行评价缺少客观标准，在 IDS 之间实现互联存在困难。单一的 IDS 产品随着技术的发展和对新攻击识别的增加，必须不断升级。

4.1.2 发展趋势

为了降低误警率、合理部署多级传感器、有效控制跨区域的传感器，下一代 IDS 产品正沿着以下几个方向发展。

1. 智能关联

将企业相关系统的信息(如主机特征信息)与网络 IDS 检测结构相融合，从而减少误警。当 IDS 使用智能关联时，它可以参考目标主机上存在的、与脆弱性相关的所有告警信息。如果目标主机不存在某个攻击可以利用的漏洞，IDS 将抑制告警的产生。智能关联包括主动关联和被动关联。主动关联是通过扫描确定主机漏洞；被动关联是借助操作系统的指纹识别技术，即通过分析 IP、TCP 报头信息识别主机上的操作系统。

2. 告警泛滥抑制

所谓“告警泛滥”是指短时间内产生的关于同一攻击的告警。告警泛滥抑制技术是将一些规则或参数(包括警告类型、源 IP、目的 IP 以及时间窗大小)融入 IDS 传感器中，使传感器能够识别告警饱和现象并实施抑制操作。传感器可以在告警前对警报进行预处理，抑制重复告警。例如，可以对传感器进行适当配置，使它忽略在 30 秒内产生的针对同

一主机的告警信息;IDS 在抑制告警的同时可以记录这些重复告警用于事后的统计分析。可以降低误警率。

新一代 IDS 产品应该能够利用一些规则对产生的告警信息进行筛选,以此来抑制告警泛滥。例如,IDS 可以根据用户需求减少或抑制短时间内同一传感器针对某个流量产生的重复告警。这样,网管人员可以专注于公司网络的安全状况,不至于因为泛滥的告警信息而大伤脑筋。

3. 告警融合

将不同传感器产生的、具有相关性的低级别告警融合成更高级别的告警信息,以便帮助解决误报和漏报问题。

当与低级别告警有关的条件或规则满足时,安全管理员在 IDS 上定义的元告警相关性规则就会促使产生高级别告警。例如,扫描主机事件,如果单独考虑每次扫描,可能认为每次扫描都是独立的事件,而且对系统的影响可以忽略不计;但是,如果把在短时间内产生的一系列事件进行整合加以考虑,则可能产生不同的结论,帮助发出早期攻击告警。通过设置元告警相关性规则,安全管理员可以把精力都集中在高级别告警的处理上。元告警相关性规则中定义的参数包括时间窗、事件数量、事件类型 IP 地址、端口号、事件顺序。

4. 可信任防御模型

改进的 IDS 中应该包含可信任防御模型的概念。2003 年开始,许多传统的 IDS 厂商已经逐渐地在 IDS 产品中增加了防御功能。从那时起,第一代入侵防御系统(IPS)产品的使用率逐渐增长。但是,IDS 产品的防御功能仍有待于提高。开发出好的内嵌防御功能的 IDS 产品的关键是提高检测的精确度。

融入可信任防御模型后,将可以解决第一代 IPS 产品遇到的问题,例如,误报导致合法数据被阻塞、丢弃;自身原因造成的拒绝服务攻击泛滥;应用级防御。

可信任防御模型中采用的机制主要有:

(1) 信任指数:IDS 为每个告警赋予一个可信值,即在 IDS 正确评估攻击/威胁后对是否发出告警的自我确信度。如对于已知的 SQLSlammer 攻击,IDS 在分析数据流中的数据报类型和大小后,以高确信度断定数据流包含 SQLSlammer 流量。因为这种攻击使用 UDP,数据报大小为 376,所用端口为 1434;有了这样的数据,IDS 会为相应的告警赋予高信任指数。

(2) DoS 攻击防护机制:攻击者可能冒充被攻击者内网中的 IP 地址(例如,邮件服务器的 IP 地址)进行欺骗攻击,传统防御系统将会拒绝所有来自邮件服务器的流量,导致网内机器不能接受外部发来的邮件,下一代 IDS 产品能够识别这种自发的 DoS 攻击,并且

降低发生概率。

(3) 应用级攻击防护机制：这是一种针对被保护力度低的应用程序(如即时通信工具、VoIP 等)发起的攻击，攻击造成的后果非常严重。下一代 IDS 产品提供深度覆盖技术来保护脆弱的应用程序免遭攻击。

4.2 网络边界防护产品——防火墙

防火墙是一个或一组系统，它们会在网络传输通过相关的访问点时对其实施一套访问控制策略。当用户确定了要提供何种水平的连接之后，就由防火墙来保证所有的网络用户都遵守访问控制策略。

防火墙的目的是控制网络传输，这一点与其他网络设备是一致的。但与其他设备不同的是，防火墙在控制网络信息传输时必须考虑到并不是所有的分组数据都是表里如一的。例如，网桥会根据分组信息的目标 MAC 地址来过滤网络传输。如果一台主机标错了目标 MAC 地址，网桥就会不可避免地把分组发送到错误的地方，这并不是网桥出错了或者不合格，而是网桥认为主机遵守了特定的网络规则，如果它没有遵守，则是主机的错误，不是网桥的错误。

目前，国际防火墙市场上分两大流派，以 Check Point 为代表的软件防火墙，在 IDC 的市场分析报告中认为其份额高达 60%以上；以 NetScreen 公司为代表的 ASIC 硬件防火墙同样不甘示弱，市场份额多年位居第三。这两类防火墙各有千秋，它们的产品发展方向也说明了未来防火墙的发展。此外，其他的一些主要厂商有：Juniper 网络公司、天融信等。

4.2.1 功能特点

目前，防火墙的类型或者其实现形式主要有以下四类：嵌入式防火墙、软件防火墙、硬件防火墙、应用程序防火墙。

1. 嵌入式防火墙

当防火墙功能被集中到路由器或者交换器中的时候，这个防火墙就称为嵌入式防火墙。这种防火墙又称为节流防火墙，通常只对分组信息进行 IP 级的无状态检查，这样可以获得较高的性能，但有较高的使危险代码通过的机会。

2. 软件防火墙

软件防火墙本身又有两种不同的类型：一种是企业级防火墙用来在大型网络上执行

路由选择功能;另一种是 SOHO(如 Small Office、Home Office、小型办公、家庭办公)级。软件防火墙通常会提供全面的防火墙功能,可以安装在服务器硬件及操作系统(如 Linux、Unix 或 Windows 2000)之上。

3. 硬件防火墙

又称为设备防火墙,设计为一种总体系统。总体系统不需要复杂的安装或者配置就可以提供防火墙服务。硬件防火墙与软件防火墙相似,可以针对企业应用市场来设计,也可以针对 SOHO 环境。

4. 应用程序防火墙

应用程序防火墙经常是作为现有硬件或者软件防火墙的组件实现的。它们的主要目的是提供一种复杂的内容过滤层次,用来对在应用层传输的数据进行过滤。随着防火墙功能的提高,对于数据的过滤已经越来越多地集中到了应用层,应用程序防火墙的针对性也越来越强。

4.2.2　主要技术

目前,大多数防火墙都采用几种功能相结合的形式来保护自己的网络不受恶意传输的攻击。其中最流行的技术有:静态分组过滤、动态分组过滤、状态过滤和代理服务器。

1. 静态分组过滤

静态分组过滤使用分组报头中存储的信息控制网络传输。当过滤设备接收到分组时,把报头中存储的数据属性与访问控制策略(称为访问控制表(ACL))对比。根据对比结果的不同,决定该信息被丢弃,还是允许它通过。

静态分组过滤可以使用下列信息管理网络传输:

(1) 目标系统的 IP(Internet Protocol,网际互联协议)地址或子网。

(2) 源系统的 IP 地址或子网。

(3) 目标服务端口。

(4) 源服务端口。

(5) 标志(只用于 TCP)。

静态分组过滤是一种智能型过滤设备,它对高级攻击提供的保护很少。它只查看很少的一些信息来确定哪些传输应该放行,哪些传输应该阻塞。许多路由器都具有进行静态分组过滤的能力。

2. 动态分组过滤

动态分组过滤比静态分组过滤更进一步,它可以维护一份连接表来监视通信会话的

状态,而不是简单地依靠标志的设置。这是一种强大的功能,可以用来更好地控制网络传输流。

例如,假设一个攻击者向系统发送了一个分组,其中的数据设计用来破坏该系统。攻击者会使用一些分组欺骗手段使某个分组看起来更像是对内部系统发送的信息的回复。普通的分组过滤器会分析这个分组,发现 ACK 位为 1,并因此而上当,认为是对某个数据请求的回复,顺利地放行,使之进入内部网络。但动态分组过滤器不会这么轻易上当。当它接收到该信息时,动态分组过滤器会查找自己的连接表(有时称为状态表),查找结果表明,内部网络根本没有发出这种数据请求。由于没有明显地请求该信息,因而动态分组过滤会把它丢进垃圾站。

动态分组过滤是一种根据分组的属性和状态表进行网络传输控制决策的智能型设备。状态表使得防火墙设备可以“记录”前面发生的通信分组交换过程,并且根据这些辅助信息进行判断。

动态分组过滤的最大缺陷是不能根据实际传输的数据内容进行判断。为了对数据内容进行过滤,用户必须使用基于代理服务器的防火墙。

3. 状态过滤

状态过滤技术提高了动态分组过滤器的功能。它的状态规则是针对具体的协议的,记录着会话的上下文信息(而不仅仅是会话的状态)。这样就使得过滤规则能够区分各种无连接协议,如 UDP、NFS(Network File System,网络文件系统)和 RPC(Remote Procedure Call,远程过程调用)。由于这些无连接协议本身的特性,使得它们无法被静态分组过滤技术管理,并且也不能得到动态分组过滤技术的准确识别。

状态过滤技术最大的优势在于为动态分组过滤处理提供了维护应用程序状态的能力,而不仅仅是维护连接状态。应用程序信息可以使一位此前经过了身份验证的用户再创建新的连接而不需要重新进行授权,而连接状态则只在一个会话期间维护着授权信息。

使用这种技术的示例可以是一个防火墙,它允许根据每个用户的身份验证来确定是否允许它进行内部访问。

4. 代理服务器

代理服务器(有时称为应用程序网关或存储转发器)是一种调节两个网络段之间的信息传输的应用程序。有了代理服务器作为调节者,源系统和目标系统就永远不会直接“连接”起来。代理服务器在所有的连接尝试中都扮演中间人的角色。

与对应的分组过滤器不同,代理服务器不对任何网络传输选择路由。实际上,配置正确的代理服务器会把所有的路由选择功能关闭。正如其名称所示,代理服务器是每个系统中各方防火墙的代言人。

由于代理服务器必须“理解”使用的应用程序协议，所以它们也可以实现针对协议的安全保护。

另外，有一种不完善的代理服务器称为插入网关。它们不是真正的代理服务器，因为它们不能够理解所支持的应用程序。插入网关只能提供简单的指定服务端口连接，与动态分组过滤相比没有什么优点。

运行代理服务器客户软件有许多优点。首先是容易配置，只需要有合法的 IP 地址和子网掩码就可以配置。另外，代理服务器客户程序也可以提供透明的身份验证，以根据用户名和口令核实出站连接尝试是否合法。

4.2.3　部署

防火墙的具体部署方法要视具体情况，综合应用性能、价格和安全保障需求进行折中处理。一般地，在网络边界上和网络内部部署防火墙，需要考虑的问题明显不同。

1. 部署边界防火墙

设置边界防火墙的正确位置应该在内部网络与外部网络之间。防火墙设置在此位置上，防火墙的内外网卡分属于内部和外部网段。内部网络和外部网络被完全隔离开，所有来自外部网络的服务请求只能到达防火墙，防火墙对收到的数据包进行分析后将合法的请求传送给相应的服务主机，对于非法访问加以拒绝。内部网络的情况对于外部网络的用户来说是完全不可见的。由于防火墙是内部网络和外部网络的唯一通信信道，因此防火墙可以对所有针对内部网络的访问进行详细的记录，形成完整的日志文件。防火墙要保护的网络与外部网络应该只有唯一的连接通路，如果防火墙后还有其他通路，防火墙将被短路，无法完成保护内部网络的工作。如果内部网络有多个外部连接，就应该在每个入口处都放置防火墙。

设置边界防火墙可以有效地防范来自外部网络的攻击。设置防火墙后内部网与外部网进行了有效地隔离，所有来自外部网络的访问请求都要通过防火墙的检查，安全有了很大的提高。

边界防火墙可以完成以下具体任务。

通过源地址过滤，拒绝外部非法 IP 地址，有效地避免了外部网络上与业务无关的主机的越权访问，防火墙可以只保留有用的服务，将其他不需要的服务关闭，可将系统受攻击的可能性降低到最小限度，使黑客无机可乘。边界防火墙可以制定访问策略，只有被授权的外部主机可以访问内部网络的有限的 IP 地址，保证外部网络只能访问内部网络中必要的资源，与业务无关的操作将被拒绝。由于外部网络对 DMZ 区主机的所有访问都要经过防火墙，防火墙可以全面监视外部网络对内部网络的访问活动，并进行详细的记录，

通过分析可以得出可疑的攻击行为。对于远程登录的用户，如 TELNET 等，防火墙利用加强的认证功能，可以有效地防止非法入侵。安装边界防火墙后，网络的安全策略由防火墙集中管理，因此黑客无法通过更改某一台主机的安全策略来达到控制其他资源访问权限的目的。边界防火墙可以进行地址转换工作，外部网络不能看到内部网络的结构，使黑客攻击失去目标。以上内容充分说明，企业的计算机网络安装边界防火墙后，可以实现内部网络与外部网络的有效隔离，防止来自外部网络的非法攻击。同时，保证了 DMZ 区服务器的相对安全性和使用便利性。

2 部署内部防火墙

企业的计算机网络是一个多层次、多结点、多业务的网络，各结点间的信任程度较低，但由于业务的需要，各结点和服务器群之间又要频繁的交换数据。通过在服务器群的入口处设置内部防火墙，可以制定完善的安全策略，有效地控制内部网络的访问，具体可以实现以下功能。

内部防火墙可以精确制定每个用户的访问权限，保证内部网络用户只能访问必要的资源。对于拨号备份线路的连接，通过强大的认证功能，实现对远程用户的管理。内部防火墙可以记录网段间的访问信息，及时发现误操作和来自内部网络其他网段的攻击行为。防火墙通过安全策略的集中管理，每个网段上的主机不必再单独设立安全策略，降低人为因素导致的网络安全问题。

例如，如图 4-2-1 所示，天融信防火墙在某校园网络的应用中，就结合该用户的具体情况和应用需求，部署了边界防火墙、内网保护服务器群防火墙，并对原有的边界防火墙实现了再利用。

其中，边界防火墙的配置、内网保护服务器群防火墙的配置和对原有边界防火墙的再利用的具体实现方法分别如下。

边界防火墙的配置：由于在该校园网络边界处已经配备的防火墙可能不支持 TOPSEC 联动协议，因此将此防火墙更换掉用于其他网络部分，如可以放置在 9、10 层计算机实验室的出口处用于保护学生上网时对教学区、图书馆网络的非法访问。根据网络具体流量情况，采用型号为 NGFW4000，支持 TOPSEC 联动协议，标准配置三接口的防火墙，其最大并发连接数将近 60 万个，其中两个接口分别接外网和内网两个网段，第三个口可以作为预留。

内网保护服务器群防火墙的配置：整个校园网中的资源信息服务器群是整个网络数据保护的关键，因此必须在其级联的 P333T 交换机与核心交换机 P550R 处配备一台能够支持 TOPSEC 联动协议的、高性能天融信网络卫士防火墙 4000 系统，用于对内部服务器群的访问和联动保护。此处建议采用型号为 NGFW4000-S 标准配置三个接口的防火

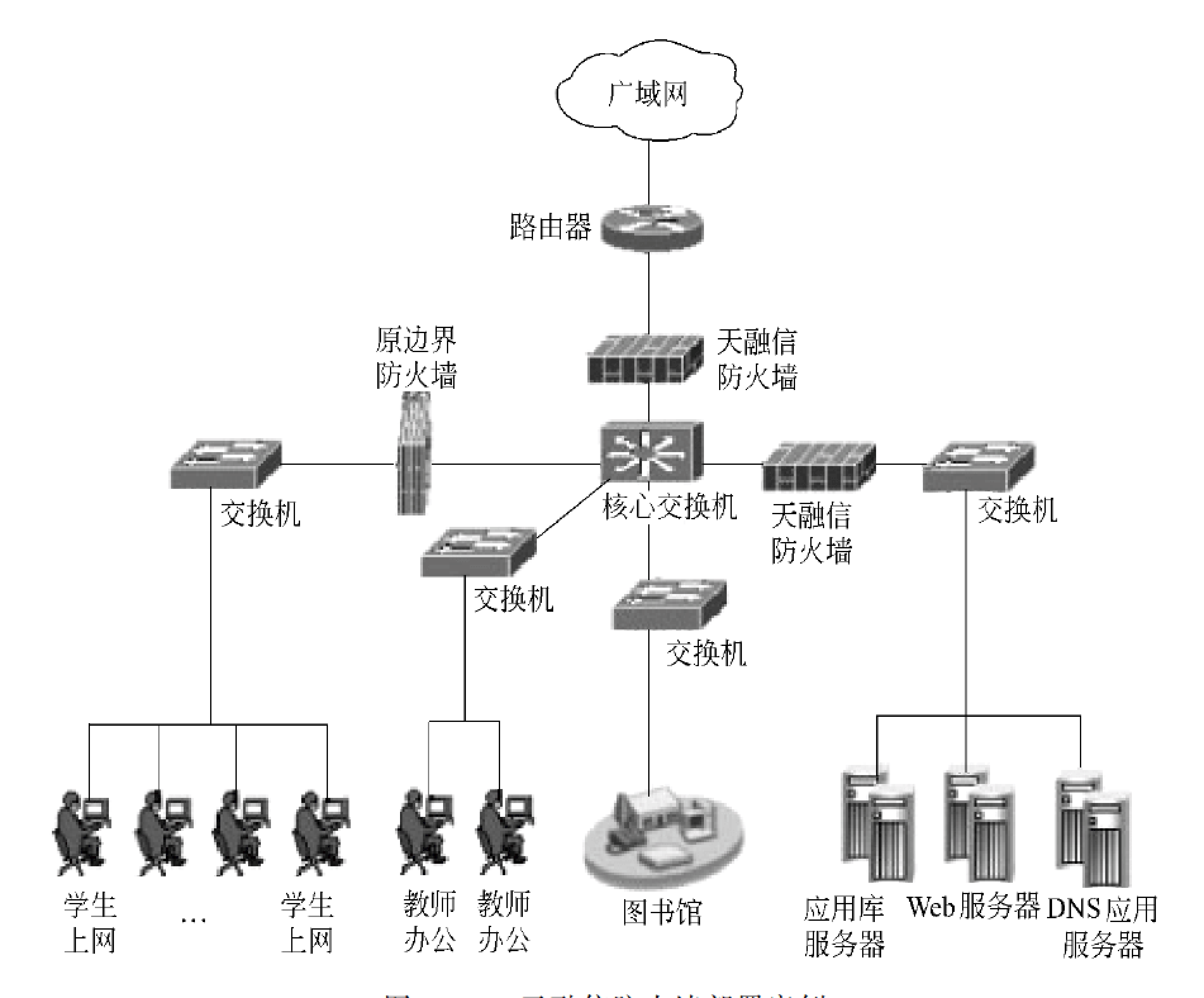


图 4-2-1　天融信防火墙部署案例

墙,其最大并发连接数达到 60 万个,一个接口接核心交换机,一个接口接级联交换机,另一个接口作为预留接口。从而实现对内部服务器群的访问控制保护。

对原有边界防火墙的再利用:由于原来的边界防火墙不支持 TOPSEC 联动协议,把它替换后可以将其放置在 9、10 层的计算机实验室网络的出口处,用于保护其对教学网和图书馆网络系统的访问控制。

4.2.4　局限性

虽然防火墙在网络安全中的应用越来越广泛,但是防火墙并不是万能的,它有很多先天的局限性,例如:

(1) 不能防范不经过防火墙的攻击。没有经过防火墙的数据,防火墙无法检查。

(2) 不能解决来自内部网络的攻击和安全问题。防火墙可以设计为既防外也防内,谁都不可信,但绝大多数单位因为不方便,不要求防火墙防内。

(3) 不能防止策略配置不当或错误配置引起的安全威胁。防火墙是一个被动的安全策略执行设备,就像门卫一样,要根据政策规定来执行安全,而不能自作主张。

(4) 不能防止可接触的人为或自然的破坏。防火墙是一个安全设备,但防火墙本身必须存放于一个安全的地方。

(5) 不能防止利用标准网络协议中的缺陷进行的攻击。一旦防火墙准许某些标准网络协议,防火墙不能防止利用该协议中的缺陷进行的攻击。

(6) 不能防止利用服务器系统漏洞所进行的攻击。黑客通过防火墙准许的访问端口对该服务器的漏洞进行攻击,防火墙不能防止。

(7) 不能防止受病毒感染的文件的传输。防火墙本身并不具备查杀病毒的功能,即使集成了第三方的防病毒软件,也没有一种软件可以查杀所有的病毒。

(8) 不能防止数据驱动式的攻击。当有些表面看来无害的数据邮寄或复制到内部网的主机上并被执行时,可能会发生数据驱动式的攻击。

(9) 不能防止内部的泄密行为。防火墙内部的一个合法用户主动泄密,防火墙是无能为力的。

(10) 不能防止本身的安全漏洞的威胁。防火墙能保护别人有时却无法保护自己,目前还没有一家厂商能绝对保证防火墙不会存在安全漏洞,因此对防火墙也必须提供某种安全保护。

此外,防火墙还具有一些脆弱性,例如:

(1) 防火墙的操作系统不能保证没有漏洞。目前还没有一家防火墙厂商说,其防火墙没有操作系统。有操作系统就不能绝对保证没有安全漏洞。

(2) 防火墙的硬件不能保证不失效。所有的硬件都有一个生命周期,都会老化,总有失效的一天。

(3) 软件不能保证没有漏洞。防火墙软件也是软件,是软件就会有漏洞。

(4) 无法解决 TCP/IP 等协议的漏洞。防火墙本身就是基于 TCP/IP 等协议来实现的,就无法解决 TCP/IP 操作的漏洞。

(5) 无法区分恶意命令还是善意命令。有很多命令对管理员而言,是一项合法命令,而在黑客手里就可能是一个危险的命令。

(6) 无法区分恶意流量和善意流量。一个用户使用 PING 命令,用作网络诊断和网络攻击,从流量上是没有差异的。

(7) 安全性与多功能成反比。多功能与防火墙的安全原则是背道而驰的。因此,除非确信需要某些功能,否则,应该功能最小化。

(8) 安全性和速度成反比。防火墙的安全性是建立在对数据的检查之上,检查越细越安全,但检查越细速度越慢。

(9) 多功能与速度成反比。防火墙的功能越多,对 CPU 和内存的消耗越大,功能越

多，检查的越多，速度越慢。

(10) 无法保证准许服务的安全性。防火墙准许某项服务，却不能保证该服务的安全性。准许服务的安全性问题必须由应用安全来解决。

4.2.5　发展趋势

防火墙技术已经从包过滤防火墙和应用网关防火墙步入状态检测防火墙。未来防火墙技术的发展趋势包括：使用网络处理器等专用硬件构建高性能网络安全计算平台，从而满足吉比特网络带宽的性能需求；从简单的 IP 端口过滤向更高层协议的应用防护方向发展，结合入侵检测技术对数据包进行有状态的深度检测；采用分布式防火墙技术对内部网络进行划分，对每个相对独立的区域实施独立的安全策略和访问控制机制等。

未来防火墙的发展趋势是向高速、多功能化、更安全的方向发展。

从国内外历次测试的结果都可以看出，目前防火墙一个很大的局限性是速度不够高。应用 ASIC、FPGA 和网络处理器是实现高速防火墙的主要方法，其中以采用网络处理器最优，因为网络处理器采用微码编程，可以根据需要随时升级，甚至可以支持 IPv6，而采用其他方法就不那么灵活。

如果要实现高速防火墙，算法也是一个关键，因为网络处理器中集成了很多硬件协处理单元，因此比较容易实现高速。对于采用纯 CPU 的防火墙，就必须有算法支撑，例如 ACL 算法。目前有的应用环境，动辄应用数百乃至数万条规则，没有算法支撑，对于状态防火墙，建立会话的速度会十分缓慢。

受现有技术的限制，目前还没有对应用层进行高速检测的有效方法，也没有任何一款芯片能做到这一点。因此，防火墙不适宜于集成内容过滤、防病毒和 IDS 功能(传输层以下的 IDS 除外，这些检测对 CPU 消耗小)。对于 IDS，目前最常用的方式还是把网络上的流量镜像到 IDS 设备中进行处理，这样可以避免流量较大时造成网络堵塞。此外，应用层漏洞很多，攻击特征库需要频繁升级，对于处在网络出口关键位置的防火墙，如此频繁地升级也是不现实的。

这里还要提到日志问题，根据国家有关标准和要求，防火墙日志要求记录的内容相当多。随着网络流量越来越大，数据规模庞大的日志记录对日志服务器提出了很高的要求。目前，业界应用较多的 SYSLOG 日志，采用的是文本方式，每一个字符都需要一个字节，对防火墙的带宽也是一个很大的消耗。二进制日志可以大大减小数据传送量，也方便数据库的存储、加密和事后分析。所以，支持二进制格式和相应的日志数据库，是未来防火墙日志和日志服务器软件的一个基本要求。

多功能也是防火墙的发展方向之一。鉴于目前路由器和防火墙价格都比较高，组网环境也越来越复杂，一般用户总希望防火墙可以支持更多的功能，满足组网便捷和节省投

资的需要。例如,防火墙支持广域网口,并不影响安全性,但在某些情况下却可以为用户节省一台路由器;防火墙支持部分路由器协议,如路由、拨号等,可以更好地满足组网需要;防火墙支持 IPSec VPN,可以利用 Internet 组建安全的专用通道,既安全又节省了租用或者自建专线的投资。

未来防火墙的操作系统会更安全。随着算法和芯片技术的发展,防火墙会更多地参与应用层分析,为应用提供更安全的保障。

4.3 网络连接防护产品——安全路由器

在安全路由器市场上,目前的主要厂商有:面向大型用户的思科、华为、3COM,以中小型用户为主的深圳市欣朗润通讯技术有限公司(开发阿尔法产品系列)。这些厂商的产品具有一个共同点,那就是:逐渐地融合了防火墙功能,或者网络管理功能。

4.3.1 局限性

安全路由器产品的局限性主要体现在传统的路由器产品的局限性方面。

路由器分本地路由器和远程路由器,本地路由器是用来连接网络传输介质的,如光纤、同轴电缆、双绞线;远程路由器是用来连接远程传输介质,并要求相应的设备,如电话线要配调制解调器,无线要通过无线接收机、发射机。

一般地,路由器具有判断网络地址和选择路径的功能,能在多网络互联环境中,建立灵活的连接,可用完全不同的数据分组和介质访问方法连接各种子网,只接受源站或其他路由器的信息,属网络层的一种互联设备。因此,它不关心各子网使用的硬件设备,但要求运行与网络层协议相一致的软件。

选择最佳路径的策略即路由算法是路由器的关键所在,这主要通过路径表(routing table)实现。路径表中保存子网的标志信息、网上路由器的个数和下一个路由器的名字等内容。路径表可以是由系统管理员固定设置好的,也可以由系统动态修改,可以由路由器自动调整,也可以由主机控制。路径表主要有两类:

1)静态路径表

由系统管理员事先设置好固定的路径表称之为静态(static)路径表,一般是在系统安装时就根据网络的配置情况预先设定的,它不会随未来网络结构的改变而改变。

2)动态路径表

动态(dynamic)路径表是路由器根据网络系统的运行情况而自动调整的路径表。路由器根据路由选择协议(routing protocol)提供的功能,自动学习和记忆网络运行情况,在

需要时自动计算数据传输的最佳路径。

路由器的优点是：适用于大规模的网络；复杂的网络拓扑结构，负载共享和最优路径；能更好地处理多媒体；安全性高；隔离不需要的通信量；节省局域网的频宽；减少主机负担。

路由器的缺点是：不支持非路由协议，安装复杂，价格高。

4.3.2 发展趋势

安全路由器产品的发展与传统的路由器产品的发展主要具有三个共性，分别是：

1. 速度更快

近几年对路由器的研究重点体现在提高路由器的处理速度上。1996—1997 年间，美国出现了一批极具创新精神的小公司，如 Nexabit、Juniper、Avici 等，把路由器的处理速度提高到了登峰造极的地步，连 Cisco 公司在速度方面都只能望其项背。由于这些高速路由器无一例外地都引入了交换的结构，因此它们也被称作吉比特交换路由器(Gigabit Switch Router，GSR)。这些路由器的光接口速度也很快从 OC-12(622Mb/s)升到 OC-48(2.5Gb/s)，再升到 OC-192(10Gb/s)，把 ATM 交换机远远地甩在后面，旷日持久的 IP 与 ATM 技术之争终于以 IP 占压倒性的优势结束。两种优秀的技术逐渐开始融合。

IP 路由器速度的急剧提高来源于以下四个方面的技术进展：

1）硬件体系结构的改进

路由器的硬件体系结构大致经历了 6 次变化，从最早期的单总线、单 CPU 结构发展到单总线、多 CPU 再到多总线多 CPU。到现在，高速 IP 路由器中多借鉴 ATM 的方法，采用交叉开关方式实现各端口之间的线速无阻塞互连。高速交叉开关的技术已经十分成熟，在 ATM 和高速并行计算机中早已得到广泛的应用，市场上可直接购买到的高速交叉开关的速率就高达 50Gb/s。伴随着高速交叉开关的引入，也同时引入了一些相应的技术问题，特别是针对 IP 多播、广播以及服务质量(QoS)，采用成熟的调度策略和算法，这些问题都得到了很好的解决。

2）ASIC 技术的采纳

出于成本和性能的考虑，这些年 ASIC 应用越来越广泛。在网络设备这一领域，出现了“可编程 ASIC”。目前，有两种类型的所谓“可编程 ASIC”。一种以 3COM 公司的 FIRE(Flexible Intelligent Routing Engine)芯片为代表，这颗 ASIC 芯片中内嵌了一颗 CPU，因而具有一定的灵活性；另一种以 Vertex Networks 的 HISC 专用芯片为代表，该芯片是一颗专门为通信协议处理的 CPU，其体系结构的设计专门适应协议处理，通过改

写微代码，可使这颗专用芯片具有处理不同协议的能力，以适应类似从 IPv4 到 IPv6 的变化。

3）3 层交换技术的出现

这是协议处理过程的一次革命性突破，也是现在 GSR 和 TSR 名称的来源。自从名不见经传的 Ipsilon 公司在 1994 年推出“一次路由，然后交换”的 IP Switch 技术之后，各大公司纷纷推出自己专有的 3 层交换技术。如 Cisco 的 Tag Switch、3Com 的 Label Switch 等。综合这些专有技术的优点，IETF 终于在 1998 年推出了性能优越的多协议标记交换（MPLS）。

4）IP over SDH，IP over DWDM

这方面的技术进展完全源于光纤通信技术的进展。随着 IP 的核心地位逐渐被认同，IP over ATM，然后 ATM over SDH 的方式被 IP 直接 over SDH 的方式取代。SDH 采用时分复用的方式承载多路数据。因此在核心网中需大量采用复用器交叉连接器，DWDM（密集波分复用）使得一根光纤上可用不同的波长传送多路信号。

2 提升服务质量

路由器在速度上的提高仍只不过是为了适应数据流量的急剧增加。而路由器发展趋势更本质、更深刻的变化是：以 IP 为基础的包交换数据将在未来几年内迅速取代已发展了近百年的电路交换通信方式，成为通信业务模式的主流。这意味着，IP 路由器将逐步提供原电信网络所提供的种种业务。但是传统的 IP 路由器并不关心也不知道 IP 包的业务类型，一般只是按先进先出的原则转发数据包，语音电话、实时视频、因特网浏览等各种业务类型的数据都被不加区分地对待。由此可见，IP 路由器要想提供包括电信、广播在内的所有业务，提高服务质量是其关键。

3. 管理更加智能化

随着网络流量的爆炸式增长和网络规模日益膨胀，以及对网络服务质量的要求越来越高的情况，各厂家网络管理的一个重要发展趋势是向智能化方向发展，主要体现在两个方面，一是网络设备（路由器）之间信息交互的智能化；二是网络设备与网络管理者之间信息交互的智能化。其中，“基于策略的管理”和“流量工程”这两个技术最引人注目。

“基于策略的管理”将同时影响路由器之间和路由器与网络管理者之间的信息交互行为模式，使网络管理者更易于从用户的角度去定义和约束网络行为，而这些上层策略将直接影响网络基本行为，使传统的路由算法发展为基于策略的路由算法，也使路由器之间的信息交互必须包含相应的策略内容。

“流量工程”是核心网运营商最关心的问题。新的协议如 MPLS 在解决标记交换的

同时,也提供了一个很好的解决"流量工程"的方法,即通过路由器之间交互各端的流量状态等信息,用收敛算法计算一段时间内网络中标记的显式路径,约束最短路径优先算法被采用以使整个网络的流量在每一段时间内尽量保持均衡。

4.4 网络连接防护产品——安全网关

4.4.1 功能

网关(gateway)是连接两个协议差别很大的计算机网络时使用的设备。它可以将具有不同体系结构的计算机网络连接在一起。在 OSI/RM 中,网关属于最高层(应用层)的设备,分为两类:面向连接的网关和无连接的网关。当两个子网之间有一定距离时,往往将一个网关分成两半,中间用一条链路连接起来,我们称之为半网关。面向连接的网关用于虚拟电路网络的互联,例如,实现 X.25 与 X.75 协议间的互联。无连接的网关用于数据报网络的互联。

安全网关是在传统网关设备的基础上侧重实现网络连接中的安全性,在功能上体现为实现内容过滤、邮件过滤、防病毒等。

目前,国内外已有很多安全网关生产厂商和产品,我国主要的安全网关生产厂商有:冠群金辰、卓尔伟业、上海格尔等。

例如,上海格尔软件股份有限公司开发的格尔 SSL 安全认证网关是一台独立网关型服务器设备,它将应用服务器隔离在一个私有网段,采用数字证书进行双向的身份认证,在客户端与服务端之间建立 128 位的加密安全通道,实现客户端和服务端的数据安全传输和客户身份的有效认证。

冠群金辰公司专为企业级用户设计的网关级安全过滤设备 KILL 过滤网关(KILL Shield Gateway,KSG),可以全面防范计算机病毒传播、阻断蠕虫攻击、拦截垃圾邮件、控制网络非法访问。它采用多层过滤(网络层、传输层、应用层)、深度内容分析、智能关联等技术策略,基于 HTTP、FTP、SMTP、POP3 等标准协议对网络数据进行过滤,可有效提升网络环境的安全状况,为业务持续运行提供有力保障。根据用户的不同需要,KSG 可实现内网综合保护、关键网段保护、邮件系统保护、网络隔离等,如图 4-4-1 所示。

该产品定位在多功能的综合过滤网关,提供全面的网络内容安全保护。根据对网络数据内容的处理能力,KSG 产品型号划分为:100 型、500 型、3000 型、5000 型,可满足不同规模的用户需要。其产品功能见表 4-4-1。

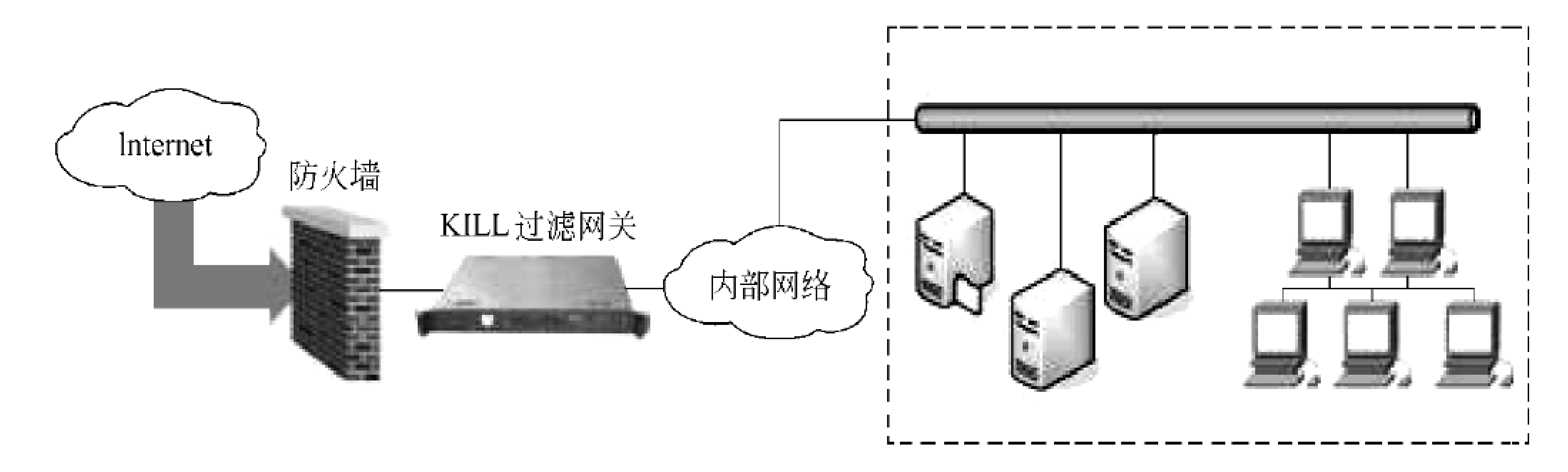


图 4-4-1 冠群金辰 KILL 过滤网关应用示意

表 4-4-1 冠群金辰 KILL 过滤网关功能

属性	功能类别	功能项	功能描述
安全特性	蠕虫过滤	蠕虫过滤	采用完整的 KILL 蠕虫库，在应用层过滤蠕虫体
		蠕虫阻断	通过对数据包的特征分析，在传输层识别和拦截蠕虫攻击
		端口封锁	可通过封锁蠕虫攻击端口方式，紧急防御大规模蠕虫爆发事件
	病毒过滤	病毒引擎	KILL 防病毒引擎
		病毒类型	邮件病毒、文件病毒、恶意网页代码、木马后门
		智能识别	深度内容分析，智能识别文件类型、压缩格式，防止伪装形式病毒
		规则过滤	可定义病毒特征和过滤规则，识别特殊病毒、未知病毒、突发病毒
	垃圾邮件过滤	规则过滤	依据 IP 地址、邮件地址、域名、邮件大小、群发数量、邮件跳数、邮件嵌套、附件数量、附件类型、文件名等进行过滤
		智能过滤	MIME 编码检查、FRC821 规范检查、HELO 标志分析、DNS 反查、自动禁止 Open Relay、贝叶斯技术、智能识别垃圾文本
		黑白名单	RBL、邮件黑名单、IP 白名单
		SMTP 认证	通过 SMTP 认证识别邮件来源，避免大量转发垃圾邮件
		伪装邮件检查	通过邮件地址和邮件用户绑定方式，确保发件的真实性
		邮件隔离	提供可疑邮件隔离功能，最终用户可从隔离区找回或彻底删除邮件
	内容过滤	关键字过滤	对邮件主题、发件人、收件人、正文、附件等进行关键字过滤
		URL 过滤	可定义 URL 地址黑白名单，禁止或允许对某些网页的访问
	网络防御	包过滤	实现基于源/目的 IP 地址、源/目的端口、协议的数据包过滤
		连接限制	并发连接限制、连接速率限制、连接频率限制
		带宽保护	动态异常流量控制技术优化网络性能，限制带宽资源占用

续表

属性	功能类别	功能项	功 能 描 述
网络特性	工作模式	连接方式	透明模式(串联)
	支持协议	网络协议	IP
		传输协议	TCP、UDP、ICMP
		应用协议	SMTP、POP3、FTP、HTTP
管理特性	系统管理	配置管理	采用 B/S 结构,支持 HTTPs 方式的 Web 管理
		在线帮助	在配置管理过程中,提供在线帮助功能
		系统维护	支持 SSH 方式的远程维护管理
		状态监视	可实时监视系统运行状态、系统负荷、过滤状态
	日志审计	日志记录	KSG 全面记录多种日志信息,定期或按需下载到日志报表系统
		日志分析	提供基于 IP/邮件地址、协议、威胁、规则、时段等过滤分析报告
		独立报表系统	采用独立工作的日志报表系统,最大限度保证 KSG 网关过滤效率
		报警	对安全威胁事件和违反策略的行为进行报警,可邮件通知管理员
	系统更新	特征码升级	病毒库、蠕虫库、垃圾邮件规则库自动更新
		系统升级	支持系统内核的在线升级
		升级方式	支持 FTP、HTTP 升级方式(通过 Internet 从冠群金辰服务器更新)

4.4.2　发展趋势

安全应用不仅要求安全产品可以满足客户目前的需要,而且还要求它们能够在安全问题迅速变化的未来及时适应新的需求。从国际安全技术发展趋势看,安全网关的未来发展有如下几个特点:

(1) 结合专用操作系统。为了持续发展自家产品,并充分发挥公司长期的知识积累,国际上大的安全厂商一般都有专业的操作系统,如 Cisco 的 IOS;Juniper (Netscreen)防火墙系列产品使用操作系统 Screen OS,NOKIA 公司的 IP 系列产品使用自己的 IPSO。设计使用专用的操作系统,目的是能为客户提供更专业更安全的系统,并能逐步发展一些核心的技术,从而拥有知识产权上的优势,自己专用的系统可以方便未来为适应新的需求进行定制化的需要。

(2) 硬件化和芯片化。软件形态的网关也逐步被硬件形态的产品代替,新兴防垃圾邮件和防病毒的网关也大都以硬件的方式出现。例如,传统的 Checkpoint 公司通过和

NOKIA 的合作来提供软硬一体的防火墙产品。为获得更高的性能，传统的基于 CPU 的软件数据处理方式也在向由芯片处理或网络处理器进行处理的方向发展。信息安全产业的高速发展，吸引了一些大的芯片厂商的关注，对于系统资源消耗比较大的计算也都改由一些高速芯片进行处理。例如，在某些 CPU、NPU 或 ASIC 芯片中就直接集成了加解密处理模块。

(3) 硬件平台多样化。为适应各种安全需要，以及产品定位的不同，各厂家的网关产品的硬件平台出现了多样发展的趋势，有基于通用 CPU 的 x86 架构的、ASIC 架构的，以及目前比较热门的基于网络处理器(NPU)架构，还有一些直接使用嵌入式芯片作为主处理器的架构，如基于 Power PC、MIPS、ARM 等嵌入式 CPU 架构的，以及采用各种技术进行组合的架构。不同的体系结构各有各的特色。

(4) 基于通用 CPU 的 x86 架构。一般采用 Intel 或 AMD 公司的芯片，x86 在架构系统时还需要北桥和南桥芯片组，采用该种硬件架构，软硬件配套资源比较多，便于快速推出产品，企业投资少，同时功能基本都由软件实现，产品比较灵活，但基于 x86 技术平台受 PCI 总线带宽和 CPU 处理能力的限制，很难满足高速环境的要求，同时 CPU 和外围芯片组发热比较大，产品寿命和稳定性难以保证。

国际上少数公司采用基于 ASIC 架构的设计，成为安全网关中的亮点。该种架构产品性能高，稳定性好，规模生产后价格比较低，但开发基于 ASIC 的产品要求的投资非常大，技术门槛高，没有一定实力的厂家很难开发这样的产品。

这几年来基于 NPU 架构来设计安全产品也成为热门话题，Intel、AMCC、Broadcom、IBM、Agere 等芯片厂商都推出了网络处理器芯片，采用 NPU 来架构安全网关，投资要比开发 ASIC 低很多，同时可以设计出比较高性能产品，但相对于 ASIC 架构，网络处理一般采用多个微引擎或多核并行处理，微引擎执行的是微码，微码具有可编程性，所以 NPU 架构要比 ASIC 架构灵活，但在稳定性上则不如主要功能由芯片来实现的 ASIC 稳定；同时 NPU 的产业标准尚需完善，产业供应链还需进一步发展。

4.5 网络连接防护产品——VPN

目前国内外已有很多 VPN 生产厂商和产品，国内主要的 VPN 生产厂商有奥联科技、深信服科技、赛蓝科技等。

4.5.1 主要技术

目前，用于企业内部自建 VPN 的主要技术有两种——IPSec VPN 和 SSL VPN，IPSec VPN 和 SSL VPN 主要解决的是基于互联网的远程接入和互连，虽然在技术上来

说，它们也可以部署在其他的网络上(如专线)，但那样就失去了其应用的灵活性，它们更适用于商业客户等对价格特别敏感的客户。

针对 IPSec VPN 和 SSL VPN 两种技术，一般认为，虽然目前企业应用最广泛的是 IPSec VPN，在未来的几年中 IPSec 的市场份额将下降，而 SSL VPN 将逐渐上升。相比较而言，二者的特点如表 4-5-1 所示。

表 4-5-1　IPSec VPN 和 SSL VPN 的对比

	IPSec VPN	SSL VPN
优点	• 能够快速完成配置 • 安全性高 • 服务质量高 • 方便拨号用户使用	• 使用方便，不需要配置，可以立即安装和使用 • 无需客户端，直接使用内嵌的 SSL 协议，而且几乎所有的浏览器都支持 SSL 协议 • 兼容性好，支持个人计算机、PDA、智能/3G 手机等一系列终端设备及大量移动用户接入的应用
缺点	• 网络不能觉察到 VPN 隧道的存在 • 具有 QoS 选项的局限 • 组建及维护成本较高	只适合 Site-to-LAN(点对网)的连接，无法解决 LAN to LAN VPN 需求

用户在考虑采用哪种技术时经常会遇到两难的选择，即安全性与方便使用的冲突。只有用户明确了自己的需求，才能选择到适合自己的解决方案。

IPSec VPN 比较适合中小型企业。这类企业拥有较多的分支机构，并通过 VPN 隧道进行站点之间的连接，交换大容量的数据。企业有一定的规模，并且在 IT 建设、管理和维护方面拥有一定经验的员工。企业的数据比较敏感，要求安全级别较高。企业员工不能随便通过任意一台计算机就访问企业内部信息，移动办公员工的笔记本计算机要配置防火墙和杀毒软件。

SSL VPN 更适合那些需要很强灵活性的企业，员工需要在不同地点都可以轻易地访问公司内部资源，并可能通过各种移动终端或设备。企业的 IT 维护水平较低，员工对 IT 技术了解甚少，并且 IT 方面的投资不多。

4.5.2　发展趋势

随着 VPN 技术的发展，其产品的发展趋势主要体现在以下几个方面。

1. 结合目录服务功能

下一代 VPN 的最主要部件是目录服务器，主要用于存放端用户的信息及网络配置数据，目录服务器决定了未来 VPN 的发展方向，它既可以运行于由 VPN 提供控制的公用网的某一部分，也可以作为运行于公司网络的一个平台。VPN 的设备与内容都可在专

用网与公用网上进行复制，公司的网络可以横跨网络公共服务设施。因此，传统公用网与专用网的界线已经变得模糊。

这些载有整个公司用户相关资料及网络配置的目录应该置于用户或网络运行中心NOC的安全区内。这个安全区是进一步开发VPN的基础，它主要由策略服务器与认证服务器组成。策略服务器根据公司的规则制定访问策略，认证服务器则负责公钥认证及其他有关安全任务。另外，VoIP网关也可以置于上述安全区内。网络如果具有上述安全机制、网络目录及服务质量(QoS)的保证，那么端用户就可以建立用于远程教育、远程医疗及虚拟会议的VPN连接了。

2. 实现QoS

为实现上述VPN，首先需要解决QoS问题。基于策略的网络提供这样一种QoS方案，策略服务器装载有关应用及网络资源的信息，动态地确定端用户如何访问应用程序。由于QoS要求提供跨越LAN与WAN的端对端的服务，增加了问题的复杂性。

在高速主干网上真正实现QoS也有很多工作有待完成。某些Internet服务提供商(Internet Server Provider，ISP)在设法将QoS提供到用户桌面。但问题是，当端用户退出某一特定电话公司的VPN时，QoS的保证也将丢失。另一个问题是，目前还没有可行的技术能够对那些跨越多个VPN的信息包进行跟踪与收费。此外，ISP还应考虑计费的可行性。

3. 安全性

安全是VPN关注的核心。目前，VPN的安全保证主要是通过使用防火墙技术、路由器并配之以网络隧道(Tunnels)、加密协议及安全密钥加以实现，这些足以保证移动端用户及远程用户安全地访问公司网络。但是，因为这需要所有的设备都必须使用相同的安全协议，实现起来非常困难。另外，认证与访问工作也都需由公司IT部门的一个中心设备所管理，因此也排除了用户动态请求加入VPN的可能，而该项功能又是外部网所必需的，随着用户的退出、加入等变动的增加，其维护开销也将增大。

上述方法将被一种灵活的、可伸缩性的、并具有互操作性的安全服务，如PKI和IKE(Internet密钥交换)技术所取代。PKI的简化版本SPKI将简化目前PKI所使用的层次验证机制。

4.6 本地环境保护产品——恶意代码防范软件

恶意代码防范软件市场是当前国内通用软件界发展的最好的一部分，市场占有率相对很高。虽然盗版软件目前还比较泛滥，但购买正版杀毒软件的用户也大有人在。目前

国内市场上的杀毒软件厂商主要有瑞星、江民、金山、诺顿、卡巴斯基、趋势等。

4.6.1 国产产品的局限性

从一些国内信息安全论坛(例如绅博、中天、安防、卡饭等)中可以看出,与国外杀毒软件产品相比,人们对国产杀毒软件的评价基本都令人失望,主要集中在以下几个方面:首先是对于新病毒和一些变种病毒的识别和杀除能力相对国外产品较差,其次是系统资源占用过高,还有就是杀毒和监测引擎不够成熟稳定,系统实时监测的速度太慢。

究其原因,除了主观因素,主要是国内厂商不能够像一些国际厂商那样拥有 Microsoft 操作系统的底层代码这一客观原因,造成了国产软件安装之后和 Microsoft 操作系统之间存在一定的兼容问题,并进一步带来了系统不稳定的问题。

由于国产杀毒软件目前对付病毒的方式主要是采用特征码方式,因此对于新病毒和变种病毒识别能力很一般。据了解,2007 版瑞星杀毒软件的引擎进行了更新,对付未知病毒的能力应该会有不小的进步。江民 2007 内置了部分 HIPS(主机入侵防御系统)功能,也可以对付部分新的威胁,但是需要用户进行判断,对用户的操作水平要求相对较高。

4.6.2 发展趋势

近年来,恶意代码防范软件经历了从单机版走向网络版,再到网关杀毒的发展。

早在 1995 年,趋势网关防毒技术就在美国申请了专利。但此后的几年,用户并没有太多关注它。后来,随着市场需求的推动,在 20 世纪 90 年代中后期,NAI、赛门铁克、趋势等国外信息安全公司的有关技术已经相当成熟,我国的冠群金辰、北信源、瑞星等厂商也推出了产品,网关杀毒市场日趋成熟。

下面介绍网关杀毒的四种实现方式。

1. 基于代理服务器的方式

此种方式主要是依靠代理服务器对数据进行还原,在数据通过代理服务器时将其数据根据不同协议进行还原,再利用其安装在代理服务器内的扫描引擎对其进行病毒的查杀。

2 基于防火墙协议还原的方式

此种方式主要是利用防火墙的协议还原功能,将数据包还原为不同协议的文件,然后传送到相应的病毒扫描服务器进行查杀,扫描后再将该文件传送回防火墙进行数据传输。病毒扫描服务器可以有多个,防火墙内的防病毒代理根据不同协议,将相应的协议数据转送到不同的病毒扫描服务器。一般来讲,不同厂商在防火墙与病毒扫描服务器之间进行数据交换的过程都采用各自的协议。在这里要重点说明的是,并不是具有协议还原功能

的防火墙就支持网关防病毒产品，目前此类产品主要支持 CVP 协议的防火墙（如 Check point 防火墙等），相对优秀的产品也能支持 PIX 等其他防火墙。由于其主要支持 CVP 协议的防火墙，而国内防火墙厂商都不是基于 CVP 标准，所以此种方式的网关防病毒产品在国内尚无法大规模地应用。

3. 基于邮件服务器的方式

此种方式也可认为是以邮件服务器为网关，在邮件服务器上安装相应的邮件服务器版防病毒产品。邮件服务器版防病毒产品与以上两种方式又不相同，它主要是通过将防病毒程序内嵌在邮件系统内（邮件版防病毒程序一般是以邮件系统的一个服务而存在的），它在进出邮件转发前对邮件及其附件进行扫描并清除，从而防止病毒通过邮件网关进入企业内部。目前，邮件版防病毒产品主要支持 Exchange Server、Lotus Notes 和以 SMTP 协议的邮件系统。

4. 基于信息渡船产品的方式

此种方式在网关防病毒产品中很少有人提到，原因是它本身不是一个防病毒产品，但其确实能够实现网关处的病毒防护。信息渡船俗称"网闸"，它采用 GAP 技术实现，在产品内建立信息孤岛，通过高速电子开关实现数据在信息孤岛的交换。用户只需在信息孤岛内安装防病毒模块，就可实现对数据交换过程的病毒检测与清除。目前，国内一些安全公司已有相应的产品。

上面四种实现方式虽然不同，但最终对数据进行扫描都是通过各厂商的病毒扫描引擎实现的，也就是说，与该厂商其他防病毒产品使用了相同的扫描引擎和病毒库，这也大大方便了网关防病毒产品的更新与升级。

从整体讲，网关防病毒产品只是防病毒产品家族中的一员，只能检测进出网络内部的数据。大多数初级网关防病毒产品只能针对 HTTP、FTP、SMTP 三种协议的数据进行病毒扫描，不能够支持 POP3 协议。这类网关防病毒产品无法解决整个网络的防病毒问题，并有效制止病毒在网络上蔓延，必须借助于一个有层次的、立体化的防病毒体系。

4.7 本地环境保护产品——密码机

密码机是按照一定的程序用于信息加密和解密的设备。密码机由密钥装置、信息输入装置、编码器和信息输出装置组成。加密是将输入密码机中的明文，变换成以一定代码表示的字母或数字组成的随机暗码，暗码可根据具体情况，利用通信技术设备、邮局、通信人员等任何一种手段传送，收到的暗码可用解密密钥解密。密码机要求有固定的信道，也

可以与保障线路的设备一起配套使用。

由于信息社会对网络技术的依赖,各种通信系统向数字化、综合化、智能化方向迅速发展,机密性要求正在从纯军事、外交领域进入政府、商业和其他许多民用领域,密码机的应用也随之更为普及。

在我国,市场上的密码机产品都必须事先通过国家密码主管部门的鉴定和审查,对密码机的使用也有相应的管理规定。目前我国的密码机生产厂商主要有卫士通、兴唐、联想等,密码机产品已经具有系列化的特点,自身的功能也日趋完善。同时,由于不同信息安全产品在功能上的融合,某些密码机产品已经具备了 VPN 产品或其他产品的一些功能。

4.7.1　功能模块

一般地,密码机主要有四个功能模块。

(1) 硬件加密部件:硬件加密部件的主要功能是实现各种密码算法,安全保存密钥,例如 CA 的根密钥等。

(2) 密钥管理菜单:通过密钥管理菜单来管理主机密码机的密钥,管理密钥管理员和操作员的口令卡。

(3) 密码机后台进程:密码机后台进程接收来自前台 API 的信息,为应用系统提供加密、数字签名等安全服务;密码机后台进程采用后台启动模式,开机后自动启动。

(4) 密码机监控程序和后台监控进程:密码机监控程序负责控制密码机后台进程并监控硬件加密部件,如果加密部件出错则立即报警。

此外,在其设计中还必须有一个密码机前台 API,用于给应用系统提供服务接口。应用系统通过密码机前台 API 调用其加密服务。密码机前台 API 是以标准 C 库的形式提供。目前密码机前台 API 支持的标准接口有:PKCS#11、Bsafe、CDSA 等。

密码机应能支持目前国内外常用的多种密码算法,主要有:

公钥密码算法:有 RSA、DSA、Diffe Hellman 算法,椭圆曲线密码算法等;

对称密码算法:有 SDBI、DES、IDEA、SMS4、RC4、RC5 等;

杂凑算法:有 MD5、SHA1 等。

4.7.2　分类

一般地,密码机分为客户端用户密码机和服务器端密码机,后者又可分为单机形式的密码机和分布式密码服务机。

客户端用户密码机,为单用户或多用户提供高端的密码服务,适合于政务办公应用。它通常作为密码服务器,通过 SOCKET 提供安全服务,具备多用户证书、密钥等的管理功能,为固定 G2G、G2E、G2B 安全办公应用提供低成本、高性能的安全服务。

应用层的客户端密码设备,应能达到如下性能指标:

(1) 公钥密码算法签名速度≥60 次/s。

(2) 公钥密码算法验证速度≥480 次/s。

(3) 对称密码算法加解密速度≥10Mb/s。

单机形式的密码机(又称单机形式的密码服务器)为特定的服务器提供密码服务,具有处理速度快、安全度高等特点。作为服务器端的密码设备,它应达到如下性能指标:

(1) 公钥密码算法签名速度≥2000 次/s。

(2) 公钥密码算法验证速度≥16 000 次/s。

(3) 对称密码算法加解密速度≥100Mb/s。

(4) 可存储的密钥对≥128 对。

例如,上海格尔软件股份有限公司开发的 SJW64 网络密码机,主要用于保证公网和专网上两个或多个网络之间的强身份认证及数据的安全传输,支持标准的 IPSec 协议,使用 PKI 证书认证技术,支持国密办加密芯片 SSP02-A,具备很高的安全性。

分布式密码服务机作为密码服务设备,采用分布式计算技术,可灵活地增加密码服务模块,实现性能动态地根据需求平滑扩展,且不影响上层的应用系统。具有处理速度快、稳定性高、可扩展性强等特点。适合于对速度和稳定性要求极高的服务器使用,如数据交换中心。

单机应能达到如下性能指标:

(1) 公钥密码算法签名速度≥2000 次/s。

(2) 公钥密码算法验证速度≥16 000 次/s。

(3) 对称密码算法加解密速度≥100Mb/s。

(4) 可存储的密钥对≥128 对。

例如,上海思波通讯科技有限公司开发的电子支付密码器系统,利用计算机信息加密技术,通过提供全套的密码信息,实现票据的鉴别,以代替传统的图章鉴别方式,它能够确保银行资金安全,加快资金的周转结算速度,广泛应用于银行、保险、企业及个人之间的票据鉴别处理,具有安全、方便、高效、可靠、易扩展的特点。北京三生先捷网络通讯技术有限公司开发的“安全电子邮件”产品可直接对电子邮件加解密、数字签名认证、远程加密传输的安全系统,实现了点对点相互加解密、服务器对客户端多人授权解密、一人对多人授权解密,同时保存了密保“增强版”的全部功能。

4.8 基础设施安全产品——PKI/CA

近年来,PKI 技术已经从理论研究阶段过渡到产品开发阶段,市场上也陆续出现了比较成熟的产品或解决方案。目前,国际上 PKI 的生产厂家及其产品很多,代表性的包括

Baltimore Technologies 公司的 UniCERT，Entrust 公司的 EntrustPKI5.0，VeriSign 公司的 OnSite。另外，包括一些大的厂商，如 Microsoft、Netscape 和 Novell 等，也已开始在自己的网络基础设施产品中增加 PKI 功能。

在我国，近年来，信息安全国家重点实验室、中国金融认证中心(CFCA)、长春吉大正元公司、上海格尔软件公司、北京数字证书认证中心、上海数字证书认证中心等信息安全研究机构、运营中心和厂商都开发了各自的 CA 产品。

例如，信息安全国家重点实验室开发的 LOIS PKI 系统是一套自主的、先进的、功能较为完善的、符合国际标准并能兼容自主密码算法的安全的国产 PKI 系统。在该系统中提出了一个自主的、完整的 PKI 应用模型框架；针对运营级 PKI 系统的需求，研制出支持 X.509、PKIX、PKCS 系列等标准的入侵容忍的 CA 系统；明确定义了 PKI 实体的概念，并基于面向对象的思想完成了 PKI 实体的相关分析与设计；形成了 PKI 最小互操作规范等多项 PKI 标准。

上海宇盟信息科技有限公司开发的 Unic PKI/CA™ 可用于企业级标准、高性价比的 PKI 实现方案，通过自身集成或第三方的可信任机构——认证中心(Certificate Authority，CA)，把用户的公钥和用户的标识信息(如名字、E-mail、身份证号等)捆绑在一起，为网络提供一致的网络身份认证服务，并可为零碎的、点对点的，特别是没有互操作性的解决方案，引入可管理的安全机制，提供可跨越多个应用和计算平台的一致安全性，实现“应用支撑”的功能，增强应用程序数据交换过程中的资源安全。

北京天威诚信电子商务服务有限公司开发的多服务器证书管理系统“服务器安证通”以经济有效地方式分发服务器证书，为标准的 Web 网站或整个公司提供安全服务。对于需要为内联网、外联网、Web 服务器机群配置 5 台或更多服务器，或有至多 4 个不同域名的机构，服务器安证可以在几分钟内给几十至上百台服务器颁发证书。

4.8.1　开发模式

目前主要有两种不同的 PKI/CA 开发模式：面向产品的开发模式和面向服务的开发模式。

面向产品的开发模式，即自建 PKI/CA 模式，指的是企业购买整套的 PKI/CA 软件，然后自行建立一整套相关的服务体系。在这种模式下，企业参与建立、维护、培训和运营整个 PKI 过程并对 PKI 软件所有事务负全责，其中包括系统、通信、数据库、物理安全、网络安全配置、高可靠性的冗余设计、灾难恢复等方面，也包括运营系统需要的 PKI 专家、法律、资金等方面。

面向服务的开发模式,即购买 PKI/CA 服务的模式,指的是企业利用第三方 CA 服务提供商的集成 PKI 平台,通过配置和管理,将企业端的前台与第三方高可靠性、高安全性的 PKI 后台组合在一起,对外提供证书服务。此模式下,企业的 CA 被托管在可信的第三方,复杂、专业的 PKI 核心服务及维护将交与专业的第三方 CA 完成,企业复杂的设备以及 PKI 专家、法律专家,不需要单独承担全部的投资与风险。

面向产品的自建 CA 与面向服务的托管 CA 代表着两种不同的开发模式。针对 PKI/CA 的建设,企业需要仔细研究后选择其所采取的模式。

4.8.2 发展趋势

基于产品和基于服务的两种 PKI/CA 开发模式,是 PKI/CA 产品的生产厂商采用的两种路线。美国的 VeriSign 公司、加拿大的 Entrust 公司和爱尔兰的 Baltimore 公司是全球最大的 PKI 产品/服务提供商,其中 Entrust 和 Baltimore 都是面向企业提供产品的 PKI 公司,它们为企业提供自建 PKI 产品的商业模式。VeriSign 是主要面向服务的 PKI 公司,它们则为企业提供 PKI 服务的商业模式。

由于需要由企业承担全部的投资与风险,市场上购买独立软件自建的 PKI 市场份额在迅速缩小。相对而言,采用基于服务的 PKI 服务平台,建设迅速、共享投资、分担风险,正在成为目前 PKI 的发展趋势。事实上,由于多数企业缺乏运营 PKI/CA 的经验和资金,自建的 PKI/CA 中有 40%在运营中出现了问题。

基于服务的 PKI/CA 开发模式没有上述局限性。这一点,通过 VeriSign 公司在全球市场占有率及股市表现上相对 Entrust 和 Baltimore 公司表现出的绝对优势得到了充分证明,见表 4-8-1。

在我国,自建 PKI 和基于服务的 PKI 共存着。国内重复建设 PKI/CA 的现象比较明显。由于各个地方、各个行业都希望建立自己的 PKI/CA,目前在我国基于产品的 PKI/CA 还有相当大的市场。主要的代表性企业是吉大正元。

从行业发展来看,以行政管理为依据的 PKI/CA 认证中心已经面临技术维护和经营管理上的双重困难,很多自建 PKI/CA 的实际营运处于停滞状态;而以市场方式运作的、独立的商务 PKI/CA 认证服务方式正逐渐成为主流。后一类提供 PKI/CA 服务的公司的代表是北京天威诚信公司。天威诚信是 VeriSign 的首要合作伙伴,学习吸收了 VeriSign 的技术以及运营管理经验,能够以最快的速度、最新的技术、最简便的方式、最适宜的投入,解决企业在线商务的安全问题,向企业提供纯商业的 PKI/CA 服务。

最近几年,随着无线应用的普及,PKI/CA 产品也有了新的发展,出现了无线 PKI。

表 4-8-1　基于服务的 PKI/CA 和自建 PKI/CA 的比较

成功因素	基于服务的 PKI/CA	自建 PKI/CA
经受考验的 PKI 技术	全面的 PKI，提供面向全球 24×7 服务的 PKI 服务中心，具备成百上千企业 CA 建设的经验，整个系统可以平滑升级	企业设计，建设和配置相关的支持设施，并承担全部的实施风险，软件提供商没有 PKI 运作的经验
适用于各种开放式应用系统	面向全社会的 PKI/CA 需求，充分考虑各种应用，采用开放结构及工业标准，与标准应用无缝集成	企业只关注自己的应用，常需要专门的客户端软件。一旦应用范围扩展，自建 CA 是否能够适应新的应用需求尚不可知
建设周期	无需基础建设，只需配置完成，建设时间很短。所有企业管理员操作都通过浏览器完成，员工培训时间短，相关策略和制度完善，即可开始使用	需要考虑很多基础设施方面的内容，包括：场地、服务器、数据库、CA 策略等。整体决策时间长，从装修场地、购买软硬件，到安装调试，建设周期很长，需要专业人员运营，人员培训时间也长
安全性	具有分 7 层的物理设施安全，提供生物识别访问控制、24 小时摄像检测、建筑加固、气态防火、网络入侵检测、系统安全审计、漏洞扫描、病毒防护、安全服务等内容。按照国际标准制定专业安全制度、安全策略，提供可信的雇员调查	企业需要自行考虑 CA 的物理安全以及网络安全，这种设计专业程度不高，质量不高，价格却不菲。企业自行制定 CA 运营的制度与策略，经验可能不足
可靠性	提供 24×7 的可靠服务，采用了网络线路、电源、服务器冗余设计、系统备份与灾难恢复、第三方审计。另外，服务 CA 采用客户保障计划，为服务提供保险赔偿，降低用户风险	企业自行考虑系统的可靠性，并自行承担操作风险。由于资金等原因，往往自建 CA 系统的可靠性得不到保证
可扩展性	对于企业是按需购买，无缝扩展，用户按照自己的显示需求购买证书，根据自己需求的变化，可随时变化购买数量，不用考虑证书数量增加导致系统配置的改变或升级	按规划建设。一经投资，无法收回。当证书需求超过建设规划时，企业需要自行考虑软硬件、人员、设施、数据库的升级
安全的运营构架	用合同的方式保证 PKI 后台的安全，如何分担责任以及由第三方审计	企业自己提供安全设施，必须设计自己的操作策略并付诸实施，承担全部的运营风险
满足外部电子商务的需求	可以选择自己的认证体系或者公用的认证体系。在公用的认证体系下，多有企业可以相互认证；在加入国际公共认证体系下，可以容易地与全球企业相互认证，实现与国际接轨	建立自己的认证体系。体系用在企业内部，各企业拥有各自的体系，当企业间需要相互认证时，需要解决复杂的交叉认证问题

如图 4-8-1 所示，CFCA 的手机证书就可以支持无线 PKI，提供基于 WAP 和短信息

两种方式手机证书，实现在移动商务中的身份验证、信息加密、数字签名，确保使用者能在任何地点、任何时间方便、及时、交互地进行安全接入信息与服务。

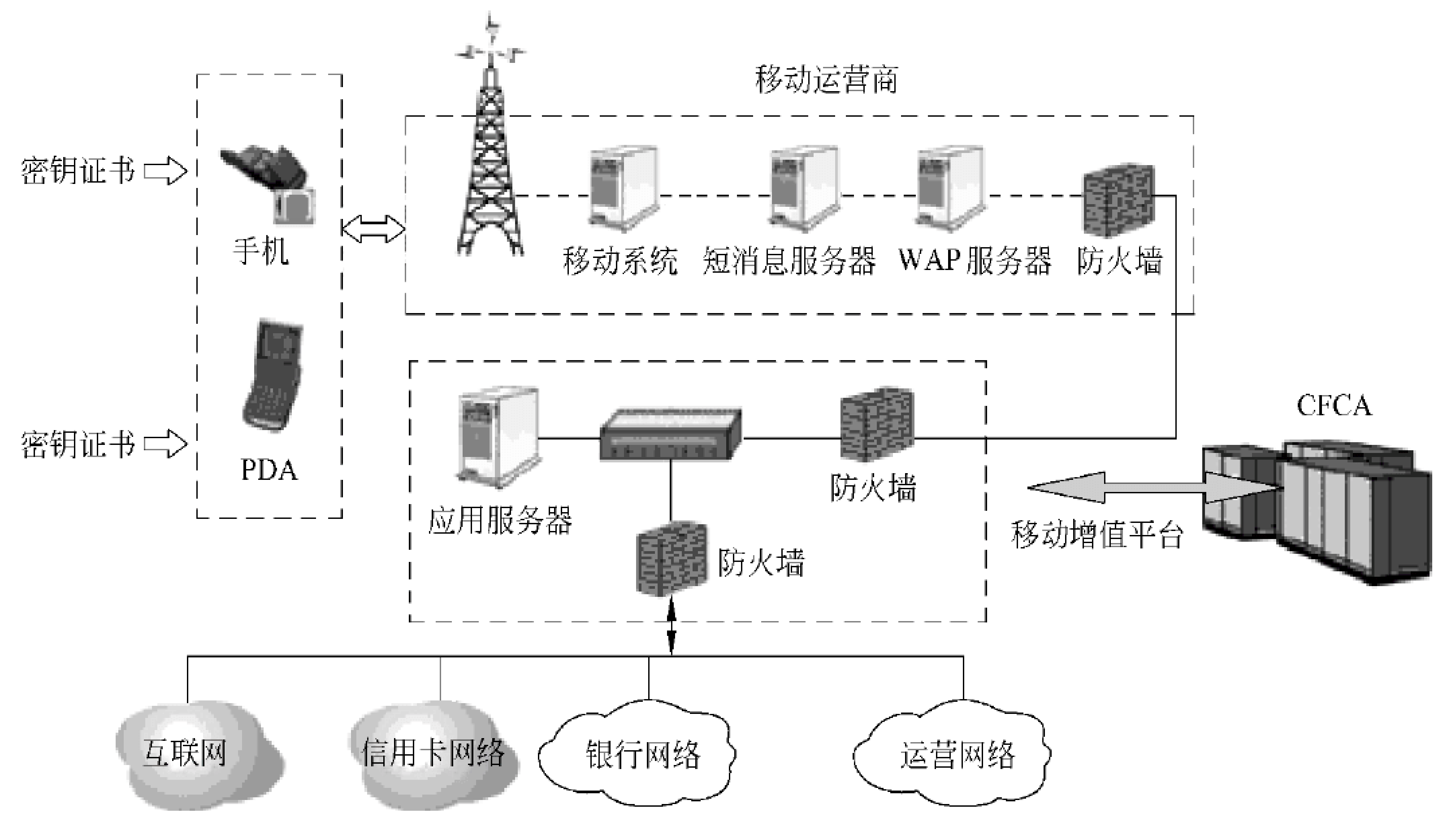


图 4-8-1 CFCA 手机证书工作示意图

移动用户以短信息的形式将请求及指令发往移动运营商(电信)，移动运营商将信息转换，使用 TCP/IP 协议发往移动商务平台，由该平台转发对应的应用服务提供商，采用证书机制能够验证移动用户、移动设备的身份、认证经加密发往各服务器的信息。

该手机证书的应用特点是：

(1) 基于 STK 和短消息(SMS)，移动用户只需与移动商务服务商单点接入，即可方便地进行注册、服务查询、账户查询、转账处理、代收付等业务。

(2) 证书与手机使用者身份绑定在一起，有效地规避了用户在移动商务中数据传输信息失真、非法篡改、否认等交易风险，极大程度地提高了无线交易的安全性。

4.9 基础设施安全产品——可信计算平台

一般来讲，可信计算的目标是通过某些专用的硬件，使计算设备如计算机更加安全。从用户的角度来讲，可信计算指通过某些机制对平台及其状态信息进行可靠的度量与报告，使得使用者确信计算平台中的软硬件环境能够按预期目标运行。从厂商的角度来讲，可信计算是一种理念，通过硬件化的平台来抵抗某些基于软件的攻击。可信计算平台

(Trusted Computing Platforms,TCP)所代表的是一系列的安全设备,如安全协处理器、密码加速器、个人令牌、可信平台模块(TPM)、增强型 CPU 等设备。

TCP 实际上是一个拥有各种保护措施的盒子,具备以下两个基本属性:能够保护数据存储区域,避免敌手直接物理上访问到机密数据存储区;能够保证系统的运行环境是安全的,没有被篡改,所有的代码能够执行于一个未被篡改的运行环境。总而言之,TCP 保护数据安全和代码安全。

可信计算的涉及面比较广,人们的认识也不尽相同,当前在信息安全领域基本认可国际 TCG 联盟关于可信计算的定义,其基本思想是在硬件平台上引入安全芯片(称作可信平台模块 TPM)架构,来提高终端系统的安全性,从而将部分或整个计算平台变为“可信”的计算平台。

4.9.1　发展历程

TCP 的发展轨迹是从安全启动发展到安全协处理器,再发展到 TPM,最后发展到 TCP。TCP 技术的思想源于早期计算机的可信启动研究。安全启动的基本思想是将系统配置分解为一系列的实体,逐一检查这些实体的完整性。

早期的安全启动系统主要有三个。1990 年研制的 Tripwire 系统,使用软件手段确保 UNIX 系统的完整性。1994 年研制的 BIT 系统,使用智能卡实现安全启动,用口令认证用户,主机和智能卡之间通过共享秘密认证,主机计算出完整性度量值和存储在智能卡的值比较后实现安全启动。1997 年研制的 AEGIS 系统,该系统基于这样的公理:BIOS 的初始化是可信的,一个组件被另一个可信组件检测验证后也是可信的。

安全协处理器的早期代表性工作主要有五项。1973 年美国国防部的 LOCK(Logical Coprocessing Kernel)项目试图使用硬件和一些相关工具,结合虚拟机监视器的原理建立一个高可信的通信子系统。1980 年 MIT 的 Stephen Kent 探索性地使用 TRM(tamper-resistant modules)保护外部软件并研制了 Kent 系统。1987 年 IBM Watson 研究院的 Steve White 和 Liam Comerford 在 Kent 系统的基础上设计了 ABYSS。1991 年 IBM Watson 研究院改进了 ABYSS 系统,形成了功能更为全面的 Citadel 系统。该系统改变了早期的 TCP 只是作为监视器或防篡改部件进行被动监视的情况,开始主动为系统提供服务。1993 年 CMU 开发了 Dyad 系统。Dyad 系统是 Citadel 系统的扩展,特别是扩展了 Citadel 系统的软件体系结构,实现了一系列应用。

关于 TPM 的标准和产品相对来说都比较成熟,TPM 标准已经发展到 1.2 版本并正在研究制定下一代 TPM 标准。当前满足标准的 TPM 产品也有很多,下面我们将会提到一些 TPM 产品及其制造商。TPM 实际上是一个含有密码运算部件和存储部件的小型片上系统(SOC),是构建可信计算平台 TCP 的基础,其体系结构如图 4-9-1 所示。

TCP 是以 TPM 为基础构建的计算平台，其可信机制主要通过三个方面来体现：

（1）可信的度量：任何将要获得控制权的实体，都需要先接受对该实体进行的度量，主要是指完整性的计算。从平台加电开始，直到运行环境的建立，这个过程就一直在进行。

（2）度量的存储：所有度量值将形成一个序列，并保存在 TPM 中，同时还包括度量过程日志的存储。

（3）度量的报告：对平台是否可信的询问正是通过“报告”机制来完成的，任何需要知道平台状态的实体，需要让 TPM 报告给它这些度量值和相关日志信息，这个过程需要询问实体和平台之间进行双向的认证。如果平台的可信环境被破坏了，询问者有权拒绝与该平台的交互或向该平台提供服务。

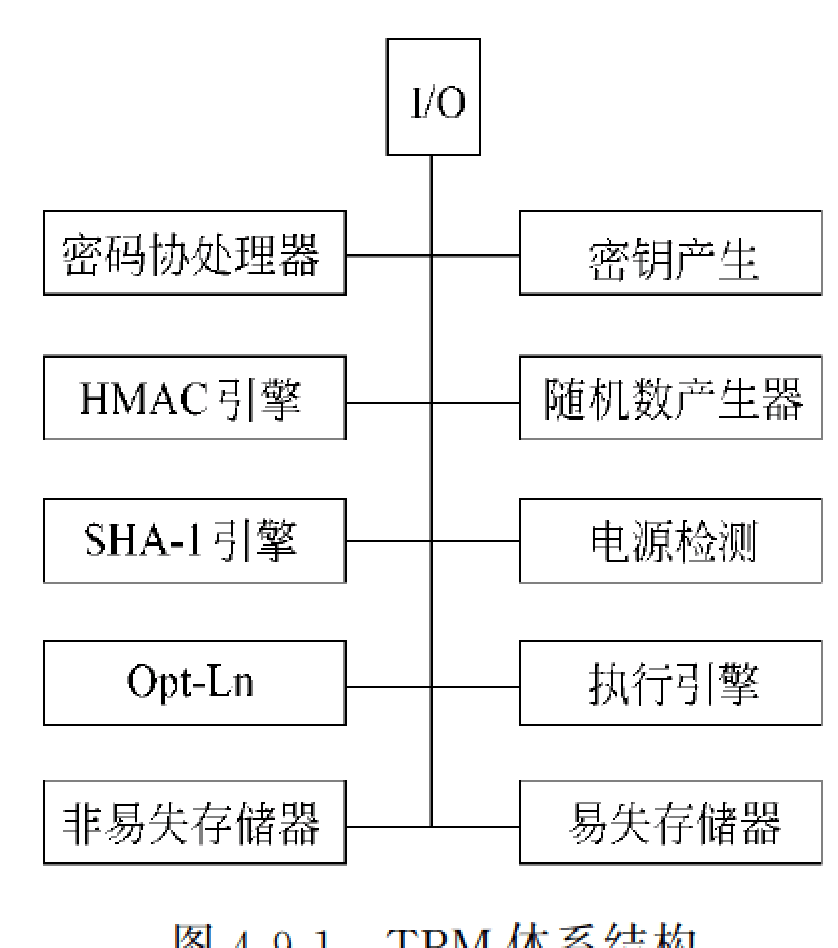


图 4-9-1　TPM 体系结构

4.9.2　发展现状

自 1999 年 IEEE 太平洋沿岸国家容错系统会议改名为“可信计算会议”，并由 IBM、HP、Intel、Microsoft 等著名企业于 2000 年 12 月 11 日成立了可信计算联盟 TCPA(2003 年改组为可信计算组织 TCG)以来，可信计算已经逐步从学术界走向产业界，全球信息技术行业几乎所有的著名公司都加入了 TCG 这一联盟组织。TCG 的宗旨是加强在相异计算机平台上的计算环境的安全性。TCG 的主要任务是通过平台、软件和技术的协作，定义、开发、推广一套开放的、系统的可信计算规范，提供一整套可信计算安全技术，规范硬件构建模块和通用的软件接口，设计多平台、多外设的可信计算环境。TCG 规范包括 TPM 规范，TCG 体系结构规范，可信软件堆栈规范，可信网络连接规范，可信客户端规范，可信服务器规范等。TCG 定义了具有安全存储和加密功能的 TPM，并于 2001 年 1 月 30 日发布了基于硬件系统的“可信计算平台规范” 1.0 版标准。该标准通过在计算机系统中嵌入一个可抵制篡改的独立计算引擎，使非法用户无法对其内部的数据进行更改，从而确保了身份认证和数据加密的安全性，2003 年 10 月发布了 1.2 版标准。

在科研方面，当前的主要研究方向集中在系统安全体系结构(包括安全启动、虚拟技术、仅执行内存(XOM)、AEGIS、Cerium)、远程证明、访问控制、数字版权管理(DRM)、生物认证、网格安全、安全增强(包括操作系统安全增强、Web 服务器安全增强、PKI 增强)等方面。

安全启动方面的研究成果有三项。Microsoft 公司的 NGSCB 技术下的安全启动功

能应用。IBM 的完整性检测系统,在 Red Hat Linux 下实现系统完整性度量,完整性度量的内容包括核心模块,可执行的共享库,配置文件等。Dartmouth 大学的 Enforcer 系统,实现了对 Linux 下的文件系统进行完整性度量。

虚拟技术方面的研究成果有 Stanford 大学的 Terra 体系结构和 Cambridge 大学的 Xen 系统。他们在技术上都采用了粒度为操作系统级的多路技术,即 TVMM 之上是多个 Guest OS,他们同时并行不悖的运行。虚拟技术的优势在于实现硬件层 TPM 的虚拟化,多个 Guest OS 同时操作 TPM,就像拥有多个 TPM 一样,并且不同的 Guest OS 之间实现了域隔离,即使一个 Guest OS 被黑客成功入侵,丝毫也不会影响其他 Guest OS 的工作。

仅执行内存(XOM)方面的研究成果有 Stanford 大学的 David Lie 和他的同事提出的基于 XOM(execute-only memory)内存的 CPU 架构。XOM 的提出是为了防止盗版以及对应用软件的恶意操作。在最后的模型中,应用程序信任 CPU 而不必信任 OS。在 XOM 结构中对程序进行加密。只有受信任的处理器拥有解密密钥。在 XOM 结构中,只有敏感的应用程序能得到这种保护。这相当于在新的特权模型中的“安全”模式。XOM 在设计时对 CPU 的结构做了适当的修改。Lie 和他的同事在 Sim OS 上开发了模拟的 XOM CPU,并且通过修改 IRIX6.5 构建了 XOMOS,在该平台上运行 MP3 播放器和 Open SSL 做测试。

MIT 的 Srini Devadas's 组在增强 CPU 的可信度方面做了很多工作,产生了新的计算机结构 AEGIS,同时在相关的支持技术方面也产生了很多成果。和 XOM 一样,AEGIS 增加了“安全”模式,增加了新的指令进入和退出安全模式,并且可以使用被保护的密钥。AEGIS 也提供了 all-or-nothing 的共享方式,内存或者受到保护环境的保护或者不被保护。与 XOM 不同的是,AEGIS 通过划分地址空间来实现这种机制,而 XOM 是通过加入数据移动的新指令来达到目的的。AEGIS 的主要应用是在 DRM 和认证执行(certified execution)上,在认证执行中,产生一个证书,证明特定的计算是在特定的处理器芯片中执行的。

Cerium 是 MIT 提出的可信处理器。Cerium 借鉴了 IBM4758 和 Dyad 的结构思想,在强化 CPU 中支持认证执行。同 XOM 和 AEGIS 一样,Cerium 利用了保护进程地址空间的方式。Cerium 借鉴了 AEGIS 组的 Merkle 树的方法。与 XOM 和 AEGIS 不同的是,Cerium 利用的是软件,它在 CPU 内部加入了可信微核。需要操作地址空间的事件引发自陷,进入微核,微核会做合适的操作。但 Cerium 目前还只停留在学术交流阶段。

远程证明是可信计算平台提供的一个核心功能。但是,现在的远程证明技术是静态的,表达能力不强,与现存的各种分布式计算环境和商业开放式系统是不相适应的。目前主要有语义、属性和软件三种远程证明技术。语义远程证明使用基于语言的虚拟机,使得远程证明具有复杂、动态和高级别程序的特点,这种特点与平台无关。California 大学实

现了语义远程证明的原型框架,提供了两个例子程序——点对点网络协议和一个分布式应用程序。属性证明不依赖于特定的软件和硬件(配置),只依赖于平台提供的"属性"。基于属性的证明应该只验证这些属性是否足够满足依赖方提出的安全需求。目前已经提出了基于属性的证明协议如何在基于 TPM 的 TC 硬件下的实现方案。软件证明是 CMU 提出的一个基于软件的证明技术(简称 SWATT)来验证嵌入式设备的内存,并且能检测到对内存内容的修改。SWATT 不需要对设备内存进行物理访问,但是仍然能提供类似于 TCG 或 NGSCB 的内存内容证明。SWATT 以很高的概率可以检测到内存内容的改变,从而检测到病毒、未预见到的配置环境和木马。

MIT 提出了基于 AEGIS 的 DRM,给出了 AEGIS 系统中的 DRM 模型。HP 实验室在网格系统中引入可信计算,增强网格结点的可信度。Dartmouth 研制了增强型安全操作系统 Enforcer,以及基于 Enforcer 的 Web Server 和 Open CA。

目前,主要的可信计算平台开源资源有 Xen 虚拟监控器,Enforcer,TrustedGrub,TPM 仿真软件,IBM 的 TPM 驱动和软件栈(TSS),IBM 可信 Linux 客户端。

在产业方面,当前的主要工作与 TCG(Trusted Computing Group)相关。

TCP 的代表技术是 Microsoft 公司的 NGSCB(Next Generation Secure Computing Base,下一代安全计算基础),Intel 的 LaGrande(Intel 在 I/O 设备方面对 TC 的支撑技术)和 ARM 的 TrustZone 技术。

可信计算平台的应用领域包括安全登录、安全 E-mail、安全 VPN 和 Web 服务、数据保护、数字签名、企业 IT 管理、安全自动升级、TPM 密钥的备份、恢复和迁移等。

国外的 TPM 制造商有 Atmel、Broadcom、Infineon、National Semiconductor 等。基于 TPM 台式机产品有 HP/Compaq 的 dc7100,IBM 的 NetVista desktops,Dell 的 OptiPlex GX520 等。基于 TPM 笔记本计算机产品有 HP/Compaq 的 nw8000,IBM 的 T43,Sony 的 VAIO BX Series 等。基于 TPM 的应用软件有 NTRU 的 Core TCG Software Stack (CTSS),IBM 的 TrouSerS 等。国内的 TPM 芯片有:联想"恒智"安全芯片,北京兆日的 SSX35 安全芯片,武汉瑞达的 SSP02 芯片。联想、瑞达等已推出基于 TPM 的安全主机产品。基于 TPM 的应用软件有信息安全国家重点实验室的 LOIS TNC 等。中国政府最近公布了《可信计算密码支撑平台功能与接口规范》,相应的技术产品也已相继问世。

4.9.3 发展方向

当前 TCP 的讨论热点主要集中在 TCG 规范,TCP 的未来设计,方法论以及 TCP 对社会的影响等方面。未来 TCP 的工作仍将沿着科研和产业两个方向展开。在科研领域,从理论上论证要达到系统可信,自芯片而上的硬件平台、系统软件、应用软件、软件开发环境、网络系统及拓扑结构所应遵循的设计策略。这一方面的研究内容仍将围绕现阶段的

主要研究课题展开。在产业界，致力于为可信计算平台构建制定工业标准，以使不同厂商的软硬件产品彼此兼容，共同营造安全可信计算环境，同时也将营造可信计算环境的思路纳入他们各自产品的设计过程之中。据 IDC 预测，2010 年几乎所有的笔记本计算机和大多数台式机都将配有 TPM 芯片。可见，TCP 有很好的发展前景。

虽然在 TCP 方面已经有很多的研究工作和可应用的产品，但仍有很多问题需要持续和创新研究，例如：

(1) 新一代可信计算平台整体架构。

(2) 高效的可信计算硬件平台。

(3) 基于可信计算硬件平台的高等级安全系统软件。

(4) 研究如何从硬件、系统及应用三个层面上实现可信存储、可信度量和可信报告。

(5) 可信计算测评技术与系统。

(6) 可信计算技术标准和规范。

4.10 安全服务产品——安全运营管理

4.10.1 安全服务产品综述

信息安全风险是整体安全风险管理战略中的重要组成部分。信息安全的发展趋势已经不仅仅是升级传统的安全产品，而是从业务策略、整体架构和完整流程方面来考虑安全问题。安全服务囊括了技术、产品、人员、过程、管理在内的各方面因素，已逐步脱离了原先依托于安全技术而生存的境地，逐渐在信息安全产业中占据主导地位，并发展成为一种全新的“产品”模式。

安全服务是引导建立信息安全整体架构和解决方案的核心内容。网络与信息系统生命周期的各个阶段都为安全服务提供了广阔的发展空间。安全咨询、风险评估、体系规划、项目实施、系统运维、安全培训、技术支持等，构成了完整的安全服务业务链。国内的金融、电信、电力等产业以及政府部门已开始成为信息安全服务的主要对象，为企事业单位的网络与信息系统提供持续、可靠、完善的安全保障。

典型的安全服务产品主要有：信息安全咨询，安全运营管理，安全体系架构规划，信息安全风险评估，应用安全评估，安全系统集成，信息安全培训等。

4.10.2 典型安全服务产品——安全运营管理

安全服务的核心是提供针对客户信息安全管理需求的完善解决方案，帮助客户更加全面地认识信息技术、评估信息安全隐患及薄弱环节，完善信息安全架构，构建安全的运

行环境，共同规划、设计、实施、运营，保护客户系统的安全。

安全运营管理是面向信息系统运行阶段的安全服务产品。由于在信息系统运行过程中，安全事件随时都可能发生，及时掌握出现的故障和存在的隐患等问题，并采取必要的应对措施，已成为保障业务系统正常运行的必要工作。针对众多企业客户面临的网络规模庞大、应用复杂、设备分散和专业技能缺乏等问题，安全运营管理服务通过统一的运营管理体系和风险管理平台，提供有效地技术、人员及流程支持，帮助客户及时地检测、响应安全事件，针对信息安全状况实施动态监控、信息整合、全局分析和决策支持。

安全运营中心（SOC）是安全运营管理服务产品的典型解决方案。通过本项服务的实施，可以协助客户构建统一、集中、高效的信息安全运营中心，调整信息安全人员组织结构，整合防火墙、防病毒、入侵检测、网络监控、主机监控、漏洞扫描等产品，整合覆盖企业全范围的信息安全监控技术架构，形成支持安全事件综合分析处理及统一管理的信息安全运营管理系统，建立企业安全管理体系和信息安全管理制度，实现企业信息安全的评估、支持、响应处理、监督、管理等功能。

4.10.3 安全服务产品发展趋势

安全服务的目标是保障客户网络及信息系统的安全，尽可能地防止、消除或降低由于信息安全事件而导致的业务损失。安全服务产品应符合最大限度提高投资回报（ROI）的基本原则，为客户提供满意的服务质量。

实践表明，成功的服务项目必须同时考虑和协调三个层面的问题：组织机构（organization）、技术（technology）、流程（process）。安全服务产品作为与 IT 技术紧密相关的一项服务产品，目前的一个主要发展趋势是与 IT 服务管理的理念相结合，把客户需求量化为安全服务所遵从的质量标准体系。

安全服务管理是基于流程和面向服务的管理过程，其目标是提高和保证安全服务质量，质量管理和流程控制形成了组织安全策略的一部分。采用 IT 服务管理方面的最佳实践——ITIL（IT 基础设施库）来规划和实施安全服务项目，可以帮助企业管理层建立以组织战略为导向，以外界环境为依据，以业务与安全整合为中心的观念，正确定位安全部门在整个组织中的作用。运用 IT 服务的管理方法能够达到既定的安全服务质量目标，履行安全服务组织和客户之间达成的服务协议。

安全服务作为一种特殊的信息技术产品，其核心是保持信息安全与企业的业务目标相一致，合理利用信息安全资源，管理信息安全风险，为推动企业的业务发展提供可靠的平台，促使企业收益最大化。通过安全服务与 ITIL 的结合，指导用户更有效地使用信息安全资源，将最佳实践与技术、产品、流程相结合，进一步体现信息安全系统对企业业务的价值，提高信息安全的投资回报率。

4.11 小结

目前市场上的信息安全产品五花八门应有尽有。但是,在真正考虑选用某种产品来满足用户的信息安全需求时,往往又会因为多种原因而不能尽快做出决定。抛开产品提供商形形色色的宣传,需要了解这些产品的真正特点、功能以及必要的性能指标。为此,本章主要以点带面地介绍了目前常见的 10 类信息安全产品,描述了他们的主要功能、特点、局限性和发展趋势,并举例说明了一些代表性产品的应用情况。

从这些产品所起的作用来看,他们主要是提供了网络边界防护、网络连接安全、本地环境安全、基础设施安全和安全服务。因此,我们把依据这些产品的主要应用环境和主要功能进行了简单归类。需要说明的是,随着产品功能的逐渐丰富,这种归类方法可能会面临一定的争议。这里的主要目的是希望这种分类能够帮助读者系统地了解信息安全产品,从而在面对真实需求的时候不忙乱、更理智。

习　　题

1. 请简要说明恶意代码防范产品的发展趋势。
2. 依据防火墙的实现形式,它可以分为哪几类?
3. 防火墙采用了哪几类技术?
4. 在网络边界上和网络内部部署防火墙,需要考虑的问题有什么不同?
5. 防火墙产品的发展趋势如何?
6. 目前的入侵检测产品具有哪些局限性?
7. 下一代入侵检测产品可能涉及哪些关键技术?
8. 什么是安全网关? 它的主要作用是什么? 技术发展趋势如何?
9. 企业内部自建 VPN 采用的两种主要技术各自有什么特点?
10. VPN 产品的发展趋势体现在哪些方面?
11. 什么是密码机? 它有哪几个主要功能模块?
12. 目前主要有哪几种不同的 PKI/CA 开发模式?
13. 请描述你所用的恶意代码防范产品的主要功能。
14. 请说明一个密码机应用实例。
15. 谈谈你对安全服务产品的认识。

第 5 章 信息安全标准

信息安全标准主要来自以下四个方面。

(1) 有关信息技术的国际标准。这些标准是由以下组织建立的：国际标准化组织(International Organization for Standardization，ISO)，国际电子技术协会(International Electrotechnical Commission，IEC)，国际电信联合会(International Telecommunication Union，ITU，原为 CCITT)和电气与电子工程师协会(Institute of Electrical and Electronics Engineers，IEEE)。

(2) 银行工业标准。这些标准或者是由 ISO 面向国际社会应用开发的，或者主要是由美国国家标准协会(American National Standards Institute，ANSI)面向美国国内的应用而开发的。

(3) 国家政府标准。这些标准是由各国政府制定的。

(4) Internet 标准。这些标准是由 Internet 协会开发的。

5.1 国际信息安全标准现状

5.1.1 国际信息技术标准化组织

目前，国际上有很多标准化组织，其中最重要的是 ISO 和 IEC，此外还包括 ITU、IETF、ECMA、IEEE 、EDTI 和 OMG 等。

ISO 和 IEC 下设机构中与信息安全标准有关的机构有：

(1) ISO/IEC JTC1 负责制定信息技术领域的国际标准，下设 19 个分技术委员会(SC)和 SGFS(功能标准化专门组)等特别工作小组，以及 4 个管理机构(分别是：一致性评定特别工作小组，信息技术任务组，注册机构特别工作组，业务分析与计划特别小组)。ISO/IEC SC27 设立于 1990 年 4 月，负责制定通用信息技术和安全技术标准。

(2) ISO/TC176 技术委员会(质量管理和质量保证技术委员会)专门研究国家质量保证领域内的标准化问题。

(3) ISO/TC97 与 SC20 分别负责数据加密技术标准化工作和密码算法国际标准化

工作。但是，由于 SC20 与 SC6 和 SC21 的工作范围有重复，SC20 于 1989 年 6 月被撤销。

(4) ISO/TC68(银行和有关的金融服务)负责制定行业应用信息安全标准。

(5) SC6(系统间通信与信息交换)主要开发系统互连下 4 层安全模型和安全协议。

(6) SC17(识别卡和有关设备)主要开发与识别卡等有关的安全标准。

(7) SC18(文件处理及有关通信)主要开发电子邮件、消息处理系统等安全标准。

(8) SC21(开放系统互连、数据管理和开放式分布处理)主要开发开放系统互连安全体系结构，各种安全框架和高层安全模型等标准。

(9) SC22(程序语言)主要开发程序语言与环境及系统软件接口的标准，同时也开发相应的安全标准。

(10) SC30(开放式电子数据交换)主要开发电子数据交换的有关安全标准。

(11) TC56(可靠性)。

(12) TC74IT(设备安全和功效)。

(13) TC77(电磁兼容)。

(14) CISPR(无线电干扰特别委员会)。

国际电信联盟(ITU)是各国电信主管部门之间协调电信事务的一个国际组织。在该组织下设的研究组中，工作内容与信息安全相关的有：

(1) SG2：负责网络与业务经营。

(2) SG4：负责电信管理网和网络维护。

(3) SG13：负责网络总体。

(4) SG16：负责多媒体业务和系统。

IETF 主要负责提出 Internet 标准草案及其意见征求稿(即 RFC)。目前有关信息安全的 RFC 已经有 170 多个。

欧洲计算机厂商协会(ECMA)主要制定计算机及其相关应用的标准和技术报告，并经常向 ISO 提交标准草案。在 ECMA 下设的 11 个技术委员会中，TC32 和 TC36 都与信息安全相关。

(1) TC32：曾经定义了开放系统应用安全结构。

(2) TC36：负责信息技术设备的安全标准，制定了商用和政府用信息技术产品和系统安全评估标准化框架，制定了开放系统环境下逻辑安全设备的框架。

5.1.2　美国信息安全标准

美国的信息技术标准主要由美国国家标准化协会(ANSI)、美国国家技术标准局(NIST)制定。此外，电子工业协会(EIA)和通信工业协会(TIA)也制定了部分信息技术标准。这些标准分为：美国国家标准、美国联邦信息处理标准(FIPS)、DoD 信息安全指令和标准(DoDDI)和 IEEE 标准。

1. 美国国家标准

ANSI 中的 NCITS 技术委员会(即 X3)负责信息技术标准,它同时也是 JTC1 的秘书处。NCITS 下设的分技术委员会 T4 负责 IT 安全技术,对应 JTC1 的 SC27。ANSI 中的 ASC X9 和 X12 负责金融安全,ASC X9 制定金融业务标准,ASC X12 制定商业交易标准。

2. 美国联邦信息处理标准(FIPS)

FIPS 在 NIST 广泛搜集政府和私人部门的意见的基础上完成,在正式发布之前,FIPS 分送给每个政府机构,经再次征求意见后,NIST 把 FIPS 标准连同 NIST 的建议一同呈送美国商务部,由部长决定同意或反对该标准。目前,已经有一系列的 FIPS 标准,而 DES 是 FIPS 安全标准中一个最著名的例子。

3. DoD 信息安全指令和标准(DoDDI)

DoD 一直非常重视信息安全,并发布了一系列有关信息安全和自动信息系统安全的指令、指示和标准。其中,DoD 5200.28-STD《国防可信和计算机系统评估准则》受到了广泛关注。

4. IEEE 标准

IEEE 在信息安全标准方面的主要贡献是提出了 LAN/WAN 安全标准 SILS 和公钥密码标准 P1363。

5.1.3 其他发达国家的信息安全标准

欧洲一些国家的信息安全标准化工作也已经开展了多年。1989 年,英国和前西德都针对安全控制可实施和安全目标不可实施进行了分类评价,后者还公布了《信息技术系统可信性评价准则》;加拿大、新西兰等国也公布了类似准则;法国、德国、荷兰与美国联合开发了《网络技术安全评价标准》的试用草案;澳大利亚、瑞士等国也在研究、制定和实施各自的信息安全标准;日本防卫厅则早在 20 世纪 80 年代就发布了《计算机安全规范》。

5.2 中国信息安全标准现状

5.2.1 工作原则与组织机构

在我国,采用国际相关标准的原则与规定如下:

(1) 采用国际标准或国外先进标准,应当符合我国有关法律和法规,保障国家安全,

防止欺骗,保护人体健康和人身、财产安全,保护动植物的生命和健康,保护环境,适合我国气候、地理条件和资源合理利用,做到技术先进,经济合理,安全可靠。

(2) 凡已有国际标准(包括即将指定完成的国际标准)的,应当以其为基础制定我国的标准,凡尚无国际标准或国际标准不能适应需要的,应当积极采用国外先进标准。

(3) 对国际标准中的安全标准、卫生标准、环境保护标准和贸易需要的标准应当先行采用,并与相关标准相协调。

(4) 我国标准采用国际标准或国外先进标准的程度分为等同采用、等效采用和非等效采用。

在我国,1984 年成立了数据加密技术分委会(后改为信息技术安全分技术委员会),2001 年成立了全国信息安全标准化技术委员会(简称信息安全标委会,TC260)。

目前,信息安全标委会下设如下工作组:

(1) 信息安全标准体系与协调工作组(WG1)。

(2) 内容安全分级及标识工作组(WG2)。

(3) 密码工作组(WG3)。

(4) 鉴别与授权工作组(WG4)。

(5) 信息安全评估工作组(WG5)。

(6) 信息安全管理工作组(WG7)。

表 5-2-1 是我国现有的一些信息安全国家标准。

表 5-2-1 2002 年前制定的信息安全国家标准(21 项)

标 准 号	标 准 名 称
GB/T 15843.1—1999	信息技术 安全技术 实体鉴别 第 1 部分:概述
GB 15843.2—1997	信息技术 安全技术 实体鉴别 第 2 部分:采用对称加密算法的机制
GB/T 15843.3—1998	信息技术 安全技术 实体鉴别 第 3 部分:用非对称签名技术的机制
GB/T 15843.4—1999	信息技术 安全技术 实体鉴别 第 4 部分:采用密码校验函数的机制
GB 15851—1995	信息技术 安全技术 带消息恢复的数字签名方案
GB 15852—1995	信息技术 安全技术 用块密码算法作密码校验函数的数据完整性机制
GB 17859—1999	计算机信息系统 安全保护等级划分准则
GB/T 17901.1—1999	信息技术 安全技术 密钥管理 第 1 部分:框架
GB/T 17902.1—1999	信息技术 安全技术 带附录的数字签名 第 1 部分:概述
GB/T 17903.1—1999	信息技术 安全技术 抗否认 第 1 部分:概述
GB/T 17903.2—1999	信息技术 安全技术 抗否认 第 2 部分:使用对称技术的机制
GB/T 17903.3—1999	信息技术 安全技术 抗否认 第 3 部分:使用非对称技术的机制
GB/T 17964—2000	信息技术 安全技术 n 位块密码算法的操作方式
GB/T 18019—1999	信息技术 包过滤防火墙安全技术要求

续表

标　准　号	标 准 名 称
GB/T 18020—1999	信息技术 应用级防火墙安全技术要求
GB/T 18238.1—2000	信息技术 安全技术 散列函数 第1部分：概述
GB/T 18238.2—2002	信息技术 安全技术 散列函数 第2部分：采用n位块密码的散列函数
GB/T 18238.3—2002	信息技术 安全技术 散列函数 第3部分：专用散列函数
GB/T 18336.1—2001	信息技术 安全技术 信息技术安全性评估准则 第1部分：简介和一般模型
GB/T 18336.2—2001	信息技术 安全技术 信息技术安全性评估准则 第2部分：安全功能要求
GB/T 18336.3—2001	信息技术 安全技术 信息技术安全性评估准则 第3部分：安全保证要求

5.2.2 信息安全标准体系框架

我国信息安全标准体系框架如图5-2-1所示。

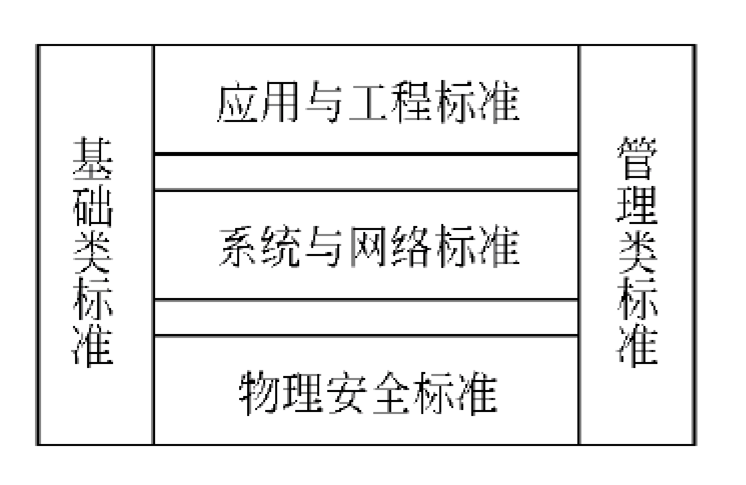


图5-2-1　我国的信息安全标准体系框架

1. 基础类信息安全国家标准

1）信息安全术语

(1) 数据处理词汇08部分：控制、完整性和安全性(GB/T 5271.8—1993；IDT ISO 2382.8-1996)。

(2) 军用计算机安全术语(GJB 2256—94)。

(3) 信息安全术语。

2）信息安全体系结构

(1) OSI安全体系结构(9387.2-1995 IDT ISO 7498-2)。

(2) TCP/IP安全体系结构(RFC 1825)。

(3) 通用数据安全体系(CDSA)。

3）信息安全框架

(1) 开放系统安全框架(ISO 10181-1)。

(2) 鉴别框架(ISO 10181-2)。

(3) 访问控制框架(ISO 10181-3)。

(4) 抗否认框架(ISO 10181-4)。

(5) 完整性框架(ISO 10181-5)。

(6) 机密性框架(ISO 10181-6)。

(7) 安全审计框架(ISO 10181-7)。

(8) 管理框架(ISO 7498-4)。

(9) 安全保证框架(ISO/IEC WD 15443:1999)。

4）信息安全模型

（1）高层安全模型(ISO 10745)。

（2）通用高层安全(ISO/IEC 11586)。

（3）低层安全模型(ISO/IEC 13594)。

（4）传输层安全模型。

（5）网络层安全模型。

5）信息安全技术

（1）加密技术。

① 算法注册(ISO/IEC 9979:1999)；

② 64 位块加密算法操作方式(GB/T 15277 IDT ISO 8372)；

③ n 位块加密算法操作方式(GB/T 17964 IDT ISO/IEC 10116)；

④ 随机比特生成(ISO/IEC WD 18031:2000)；

⑤ 素数生成(ISO/IEC WD 18032:2000)；

⑥ 密钥管理 第一部分 框架（GB 17901—1:1999 IDT ISO/IEC 11770.1:1996)；

⑦ 密钥管理 第二部分 使用对称技术的机制（GB 17901—2:1999 IDT ISO/IEC 11770.1:1998)；

⑧ 密钥管理 第三部分 使用非对称技术的机制(GB 17901—3:1999 IDT ISO/IEC 11770.1:1998)；

⑨ 分组密码算法；

⑩ 公开密钥密码算法；

⑪ 序列密码算法。

（2）签名技术。

① 带消息恢复的数据签名方案(GB/T 15852:1995 IDT ISO/IEC 9796)；

② 带附录的数字签名(GB/T 17902 IDT ISO/IEC 14888)；

③ 散列函数(GB/T 18238 IDT ISO/IEC 10118)。

（3）完整性机制。

① 作密码校验函数的数据完整性机制(GB 15852:1995 IDT ISO/IEC 9797:1994)；

② 消息鉴别码(ISO/IEC 9797)；

③ 校验字符系统(ISO/IEC CD 7064:1999)。

（4）鉴别机制。

① 实体鉴别(GB/T 15843 IDT ISO/IEC 9798)；

② 目录框架鉴别(ISO/IEC 9594-8:1997 /ITU-T X.509)；

③ 消息鉴别。

(5) 访问控制机制：安全信息对象(ISO/IEC FDIS 15816:1999)。

(6) 抗否认机制。

① 抗否认(GB/T 17903:1999 IDT ISO/IEC 13888:1998)；

② 时间戳服务(ISO/IEC WD 18014:2000)。

(7) 路由选择控制机制。

(8) 通信业务填充机制：网络层安全协议(GB/T 17963:2000 IDT ISO/IEC 11577:1995)。

(9) 公证机制。

① 可信第三方服务管理指南(ISO/IEC FDIS 14516:1999)；

② 可信第三方服务规范(ISO/IEC FDIS 15945:1999)；

(10) 可信程度。

(11) 事件检测和报警。

① IT 入侵检测框架(ISO/IEC PDTR 15947:1999)；

② 安全预警技术。

(12) 安全审计跟踪。

(13) 安全标记。

① 用户接口安全标记；

② 数据管理安全标记；

③ 数据交换安全标记；

④ 数据通信安全标记；

⑤ 操作系统安全标记。

(14) 安全恢复。

(15) 其他技术。

① PKI 技术；

② KMI 技术；

③ PMI 技术。

2 物理安全类信息安全国家标准

1) 物理环境安全

(1) 机房。

① 计算机场地通用规范(GB/T 2887:2000)；

② 计算机场地安全要求(GB 9361:1988)；

③ 计算机机房用活动地板技术条件(GB 6650—1986)；

④ 电子计算机机房设计规范(GB 50174—1993)。

(2) 计算机信息系统防雷保安器(GA 173—98)。

(3) 电磁泄露发射(TEMPST)。

① BMB 1—1994 电话机电磁泄露发射限值和测试方法(机密级);

② BMB 2—1998 使用现场的信息设备电磁泄露发射检查测试方法和安全判据(绝密级);

③ BMB 3—1999 处理涉密信息的电磁屏蔽室的技术要求和测试方法(机密级);

④ BMB 4 电磁干扰器技术要求和测试方法(秘密级);

⑤ BMB 5 涉密信息设备使用现场的电磁泄露发射防护技术要求(秘密级);

⑥ GGBB 1—1999 信息设备电磁泄露发射限值(绝密级);

⑦ GGBB 2—1999 信息设备电磁泄露发射测试方法(绝密级)。

(4) 电磁兼容(GB 9254—1988)。

(5) 电磁干扰。

(6) 电气安全。

2) 介质安全

(1) 媒体安全。

(2) 存储场地安全。

3. 系统与网络类信息安全国家标准

1) 安全协议

(1) 安全数据交换协议 IEEE 802.10。

(2) 密钥管理协议 IEEE 802.10c。

(3) 传输层安全协议(ISO 10736)。

(4) 应用层安全协议(ISO 11577)。

(5) 网络管理协议(SNMP)。

(6) IPSec 协议。

(7) XML。

2) 安全信息交换语法规则

本书略。

3) 网络平台安全标准

本书略。

4) 应用平台安全标准

(1) 数据库安全,可供参照的标准如下:

① DoDD 8320.1 美国国防部数据库管理；

② NCSC-TC-021 TESEC 对数据库管理系统的解释；

③ FIPS PUB 127-1 Database Language SQL(ANSI X3.135-1992)。

(2) Web 安全技术，可供参照的标准如下：

① RFC 2084, Considerations for Web Transaction Security;

② RFC 2068, Hypertext Transfer Protocol-HTTP/1.1;

③ The SSL Protocol Version 3.0,1996;

④ IETF-Draft, The Private Communication Technology Protocol,1995;

⑤ IETF-Draft, The Hypertext Transfer Protocol,1995。

(3) E-mail 安全技术，可供参照的标准如下：

① RFC 2311, S/MIME Version 2 Message Specification;

② RFC 2312, S/MIME Version 2 Certificate Handling;

③ RFC 2440, Open PGP Message Format;

④ RFC 1412, Privacy Enhancement for Internet Electronic Mail: Part 1:Message Encryption and Authentication Procedures;

⑤ RFC 1422, Privacy Enhancement for Internet Electronic Mail: Part 2:Certificate-Based Key Management;

⑥ RFC 1423, Privacy Enhancement for Internet Electronic Mail: Part 3:Algorithms, Modes, and Identifiers;

⑦ RFC 1424, Privacy Enhancement for Internet Electronic Mail: Part 4:Key Certification and Related Services;

⑧ IETF-Draft, Cryptographic Message Syntax;

⑨ IETF-Draft, Enhanced Security Services for S/MIME;

⑩ IETF-Draft, S/MIME Version 3 Message Specification;

⑪ IETF-Draft, S/MIME Version 3 Certificate Handling;

⑫ IETF-Draft, Certificate Distribution Specification;

⑬ IETF-Draft, Diffie-Hellman Key Agreement Method;

⑭ IETF-Draft, Domain Security Services Using S/MIME;

⑮ IETF-Draft, Examples of CMS Message Bodies。

(4) FTP 安全技术，可供参照的标准如下：

① IETF-Draft, Kerberos Change Password protocol;

② IETF-Draft, The Kerberos Network Authentication Service(v5);

③ IETF-Draft, FTP Authentication Using DSA;

④ IETF-Draft，Extension to Kerberos v5 for Additional Initial Encryption；

⑤ IETF-Draft，The Kerberos v5 GSSAPI Mechanism，Version 2；

⑥ RFC 1510，The Kerberos Network Authentication Service(v5)。

(5) SSH,可供参照的标准如下：

① IETF-Draft，SSH Protocol Architecture；

② IETF-Draft，SSH Transport Layer Protocol；

③ IETF-Draft，SSH Authentication Protocol；

④ IETF-Draft，SSH Connection Protocol；

⑤ RFC 1411,Telnet Authentication：Kerberos Version 4；

⑥ IETF-Draft，Generic Message Exchange Authentication for SSH。

(6) 电子商务,可供参照的 Internet 商务标准和 SET 标准分别是：

① The Standard for Internet Commerce，Part 1：Business to Consumer (Draft 1.0),1999；

② SET Secure Electronic Transaction Specification，Version 1.0,1997。

5) 业务应用安全

金融、证券、党政机关、军队、电信、工商、税务、社保、海关和电力等行业的业务应用安全。

4. 应用与工程类信息安全国家标准

1) 信息安全产品

(1) 包过滤防火墙(GB/T 18019)。

(2) 应用级防火墙(GB/T 18020)。

(3) 应用代理服务器(GB/T 17900)。

(4) 安全路由器(GB/T 18018)。

(5) 证书认证中心(参见《电子商务安全证书认证中心的安全要求》,中国国家信息安全测评认证中心)：

① PKCS# 1：RSA Encryption Standard. Version 1.5，Nov. 1993；

② PKCS# 3：Diffie-Hellman Key-Agreement Standard. Version 1.4，Nov. 1993；

③ PKCS# 5：Password-Based Encryption Standard. Version 1.5，Nov. 1993；

④ PKCS# 6：Extended-certificate Syntax Standard. Version 1.5，Nov. 1993；

⑤ PKCS# 7：Cryptographic Message Syntax Standard. Version 1.5，Nov. 1993；

⑥ PKCS# 8：Private-Key Information Syntax Standard. Version 1.2，Nov. 1993；

⑦ PKCS# 9：Selected Attribute Types. Version 1.1，Nov. 1993；

⑧ PKCS# 10：Certification Request Syntax Standard. Version 1.0，Nov. 1993；

⑨ PKCS# 11：Cryptographic Token Interface Standard. Version 1.0，Apr. 1995；

⑩ RFC 1777：Lightweight Directory Access Protocol，Mar. 1995；

⑪ RFC 2251：Lightweight Directory Access Protocol (v3)，Dec. 1997；

⑫ RFC 2256：A Summary of the X.500(96) User Schema for Use with LDAP v3，Dec. 1997；

⑬ RFC 2307：An Approach for Using LDAP as a Network Information Service，Mar. 1998；

⑭ RFC 1521-1522：MIME，Sep. 1993；

⑮ RFC 2312：S/MIME v2 Certificate Handling，Mar 1998；

⑯ RFC 1421-1424：Privacy Enhancement for Internet Electronic mail，Feb. 1993；

⑰ RFC 821：Simple mail Transfer protocol，Aug. 1982；

⑱ RFC 1750："随机书安全建议"；

⑲ RFC 2104："HMAC：消息认证的密钥散列"所指定的 Hash 函数；

⑳ Internet Draft：The SSL Protocol v3，Nov. 1996；

㉑ Internet Draft：Certificate Management Messages over CMS，Mar. 1998；

㉒ Internet Draft：Internet X. 509 Public Key Infrastructure：Certificate Management Message Formats，Feb. 1998；

㉓ Internet Draft：Internet X. 509 Public Key Infrastructure：Certificate Management Message Protocols，Feb. 1998；

㉔ Internet Draft：Certificate Request Message Formats，Feb. 1998；

㉕ Internet Draft：X. 509 Internet Public Key Infrastructure：Online Certificate Status Protocol，Apr. 1998；

㉖ Internet Draft：X. 509 Internet Public Key Infrastructure：Open CRL Distribution Process (Open CDP)，Apr. 1998；

㉗ Internet Draft：SPKI Requirements，Mar. 1998；

㉘ Internet Draft：SPKI，Mar. 1998；

㉙ Internet Draft：Web-Based Certificate Access protocol—Web CAP/1.0，Apr. 1998；

㉚ Internet Draft：Internet Public Key Infrastructure：X. 509 Certificate and CRL Profile，Mar. 1998；

㉛ Internet Draft：Internet X. 509 Public Key Infrastructure：Operational Protocols-FTP and HTTP。

(6) 网络密码机(包括宽带网络密码机)。

(7) 智能卡(包括 SIM 卡、金融卡),可供参照的标准如下:

① GB/T 14916—94 识别卡 物理特性(ISO/IEC 7810:1985);

② GB/T 17552—98 识别卡 金融卡交易(ISO/IEC 7813:1995);

③ GB/T 16649.1—1996 识别卡 带触点的集成电路卡 第一部分 物理特性(ISO/IEC 7816-1:1998);

④ GB/T 16649.2—1996 识别卡 带触点的集成电路卡 第二部分 触点的尺寸和位置(ISO/IEC 7816—2:1998);

⑤ GB/T 16649.3—1996 识别卡 带触点的集成电路卡 第三部分 电信号和传输协议(ISO/IEC 7816-3:1998);

⑥ ISO 7816-1 识别卡——带触点的集成电路卡;

⑦ ISO 7816-2 触点尺寸、数量、用途和位置;

⑧ ISO 7816-3 IC 卡和接口设备之间的电子信号和报文交换协议;

⑨ ISO 7816-4 行业间交换命令,IC 卡数据组织复位响应;

⑩ ISO 7816-5 应用标识符的编号体系和应用提供者标识符的注册程序;

⑪ ISO 10202 金融事务卡,使用集成电路卡的金融事务系统的安全体系结构;

⑫ ISO 14443 不带触点的集成电路卡。

(8) IC 卡(ISO/IEC 7816/7813)。

(9) 安全 PC 卡,可供参照的标准如下:

① PC CARD STANDARD RELEASE 2.1;

② FORTEZZA 应用实现者指南,MD 4002101-1.52,1996.3.5;

③ FORTEZZA 密码逻辑接口程序员指南,MD 4002101-1.52,1996.1.30。

(10) 语音保密设备,可供参照的标准如下:

① GB 4943—1995;

② FIPS 140-1;

③ GJB XXXX—XX;

④ MIMA。

(11) 数据保密设备,可供参照的标准如下:

① GB 4943—1995;

② FIPS 140-1;

③ GJB XXXX—XX;

④ MIMA。

(12) 传真保密设备,可供参照的标准如下:

文件传真机(模拟)的收发同步、合作因数、合作指数、引起错位的抖动以及跟踪载频

偏离的能力等均应以传真稿件的高保真为基础，传真接口应该可靠、安全。模拟传真机不宜用于保密要求级别高的通信，并且在使用时应该对传真信号进行二维以上的置乱掩盖。党政机关应使用保密通信要求为1～4类的传真机及其内置式装置(例如modem)。这4类传真机的技术标准分别是：

① 1类：GB 10198.1—88(等同于CCITT T.2(1976))；

② 2类：GB 10198.2—88(等同于CCITT T.3(1980))；

③ 3类：GB 10198.3—88(等同于CCITT T.4(1980))；

④ 4类：GB 10198.4—88(等同于CCITT T.563(1988))。

(13) 入侵检测产品(可参照GB/T 20275—2006)。

(14) 漏洞扫描产品(可参照GB/T 20278—2006，GB/T 20280—2006)。

(15) 安全审计产品。

(16) 身份认证产品(包括生物特征识别、一次性口令)。

(17) 安全交换机。

(18) 安全VPN，可供参照的标准如下：

① RFC 1825 Internet协议安全架构；

② RFC 1826 IP认证头；

③ RFC 1827 IP封装安全净载(ESP)；

④ RFC 1828 利用密钥化的MD5进行IP认证；

⑤ RFC 1829 ESP DES-CBC转化；

⑥ RFC 2085 利用relay防护进行HMAC-MD5 IP认证；

⑦ RFC 2104 HMAC：用于报文认证的密钥散列。

(19) 安全PC卡。

(20) 网络隔离部件(可参照GB/T 20277—2006，GB/T 20279—2006)。

(21) 防毒产品。

(22) 安全芯片。

(23) 安全操作系统(可参照GB/T 20008—2005，GB/T 20272—2006)。

(24) 安全数据库(可参照GB/T 20009—2005，GB/T 20273—2006)。

(25) 安全服务器。

(26) 风险分析系统。

(27) 安全网管系统。

(28) 中间件。

2) 安全工程与服务

(1) 系统安全工程能力成熟度模型(SSE-CMM)。

（2）安全工程质量。

（3）安全工程监理。

（4）信息安全服务资质。

3）人员资质

4）行业应用

5. 管理类信息安全国家标准

1）管理基础

（1）安全产品分类编码。

（2）信息技术安全管理指南(ISO/IEC 13335)。

（3）信息安全管理(ISO/IEC TR 17799)。

（4）计算机信息系统安全保护等级划分准则(GB 17859:1999)。

2）系统管理

（1）安全报警报告功能(GB 17143.7—1997 IDT 10164.7—1992)。

（2）安全审计跟踪功能(GB 17143.8—1997 IDT 10164.8—1992)。

（3）访问控制对象和属性(GB 17143.9—1997 IDT 10164.9—1992)。

（4）风险管理。

3）测评认证

（1）信息技术安全性评估准则(GB/T 18336 IDT ISO/IEC 15408:1999)(CC)。

（2）PP/ST 产生指南(ISO/IEC PDTR 15446:2000)。

（3）通用测评方法(SC27 N2722/CEM)。

（4）PP 注册(ISO/IEC CD 15292:2000)。

（5）系统安全工程能力成熟度模型(SSE-CMM)。

（6）安全工程质量评估准则(可参照 GB/T 20282—2006)。

（7）信息安全服务评估准则。

5.3 小结

本章介绍了国际和国内的信息安全标准工作情况，内容包括国际上的信息安全标准化组织、美国信息安全标准分类、我国信息安全标准现状和信息安全标准体系框架，重点介绍了我国的信息安全标准体系框架。希望这些内容能够帮助读者全面了解信息安全标

准化工作的概况。

习　题

1. 国际上有哪些代表性的信息安全标准化组织？
2. 美国的信息安全标准主要有哪几类？
3. 简要描述我国的信息安全标准体系框架。

第6章 信息安全管理

信息安全管理是获得信息保障能力的重要源泉,因此也是构建信息安全体系结构不可忽视的重要因素。信息安全管理把分散的技术因素、人为因素,通过政策规则协调整合成为一体,服务于信息化使命的安全目标。

信息安全管理的相关内容非常多。本节主要介绍风险评估、信息安全管理标准 ISO/IEC 17799-1:2005 和信息安全法律法规这三方面内容。

6.1 关于风险评估

6.1.1 概念

风险评估(risk assessment),也称风险分析。从风险评估因子的角度考虑,风险评估指的是对信息和信息处理设施的威胁(threat)、影响(impact)和脆弱性(vulnerability)这三个因子及三者发生的可能性进行评估。一般地,威胁以某种概率来利用脆弱性,这种概率与多种因素相关联。这些因素包括:威胁主体(威胁的来源与有关人员的素质)、攻击方法、攻击成功的时间。同时,通常是通过威胁对信息资产的影响(后果)来描述这些受保护的信息资产的价值。

威胁发生的可能性大小与威胁发生的条件密切相关。针对具体的环境,在考虑威胁发生的可能性时应考虑信息资产的脆弱性,并依据这些脆弱性对威胁发生的可能性大小进行修正。在确定风险大小的级别时,可以采用二元风险分析法测量风险。其中,“二元”指的是经过修正的威胁利用脆弱性发生的可能性和威胁对信息资产造成的后果或潜在影响(严重性)这两个因素。

从确认安全风险及其大小的角度考虑,风险评估指的是利用适当的风险评估工具,包括定性和定量的方法,确定资产风险等级和优先控制顺序。

风险评估属于组织信息安全管理体系策划的过程,是进行风险管理的基础,也是组织确定信息安全要求的途径之一。它主要基于对现有信息系统进行安全核查与分析,从信息资产价值、系统脆弱性、系统面临的威胁等方面确定存在的安全隐患和风险级别,根据

结果提交安全分析报告，作为系统需求分析和安全设计的基础，为提高系统整体安全防护能力提供重要依据。

信息系统安全评估过程也是一个系统安全需求分析的过程。风险分析可以从评估资产价值(assets)、威胁(threats)和脆弱性(vulnerabilities)级别，业务影响分析等方面评估风险级别。同时，在风险评估的过程中，要求考虑现有的安全防范机制。

风险管理是识别、控制、降低或消除安全风险的过程。该过程通过风险评估来识别风险的大小。在此基础上，通过制定信息安全方针，采取适当的控制目标与控制方式对风险进行控制，使风险被避免、转移或降至一个可被接受的水平。

风险评估的作用是明确安全需求及确定切实可行的控制措施。全面系统的风险评估是实施有效地风险管理的基础。

风险评估主要考虑：

- 信息资产及其价值；
- 对这些资产的威胁以及它们发生的可能性；
- 漏洞与脆弱性；
- 已有的安全控制措施。

风险评估可以识别组织所面临的安全风险，确定与之相应的风险控制的优先等级，明确安全需求，确定切实可行的控制措施，从而将风险控制在组织可以接受的范围之内。全面系统的风险评估是实施有效地风险管理的基础。

根据信息安全工程学和信息安全风险管理的理论，对于一个指定的信息网络系统，在信息安全风险评估的基础上，明确信息系统中所存在的各种信息安全风险，并制定相应的信息安全策略，通过信息安全管理和各种信息安全技术的实施，实现对信息系统的各种安全风险的控制，控制目标与控制方式的选择建立在风险评估的基础之上。信息安全来自“三分技术，七分管理”，风险评估是信息安全管理的重要手段，也是确定安全需求、制定安全策略、制定安全规范和实施安全方案的基础。

但是，风险的量化是一件非常复杂的工作。风险的来源、表现形式、造成的后果、发生的可能性与风险的影响都需要建立在科学的分析方法学和数学模型之上。

6.1.2 步骤

风险评估的基本步骤是：按照组织商务动作流程进行资产识别、并根据估价原则对资产进行估价。根据资产所处的环境进行威胁识别与评价。对应每一威胁，对资产或组织存在的脆弱性进行识别与评价。对已采取的安全控制进行确认。建立风险测量的方法及风险等级评价原则，确定风险的大小与等级。

风险评估过程由输入(input)、过程(process)和输出(output)三个环节构成。其中，

这三个环节的具体内容分别是：

（1）输入：资产识别与估价，威胁识别与评价，脆弱性识别与评价，对已采取的安全控制进行确认。

（2）过程：风险评估、原则、测量与等级划分。

（3）输出：风险控制。

在进行风险评估时，应考虑的对应关系主要是资产与威胁的对应关系。每一项资产可能存在多个威胁。威胁的来源可能不止一个，应从人员（包括内部与外部）、环境（如自然灾害）、资产本身（如设备故障）等方面加以考虑。每一威胁可能利用一个或数个脆弱性。这种对应关系可以表述如下：

资产：威胁 I →[来源 I | 脆弱性 I]

风险评估中各个要素之间的关系如图 6-1-1 所示。

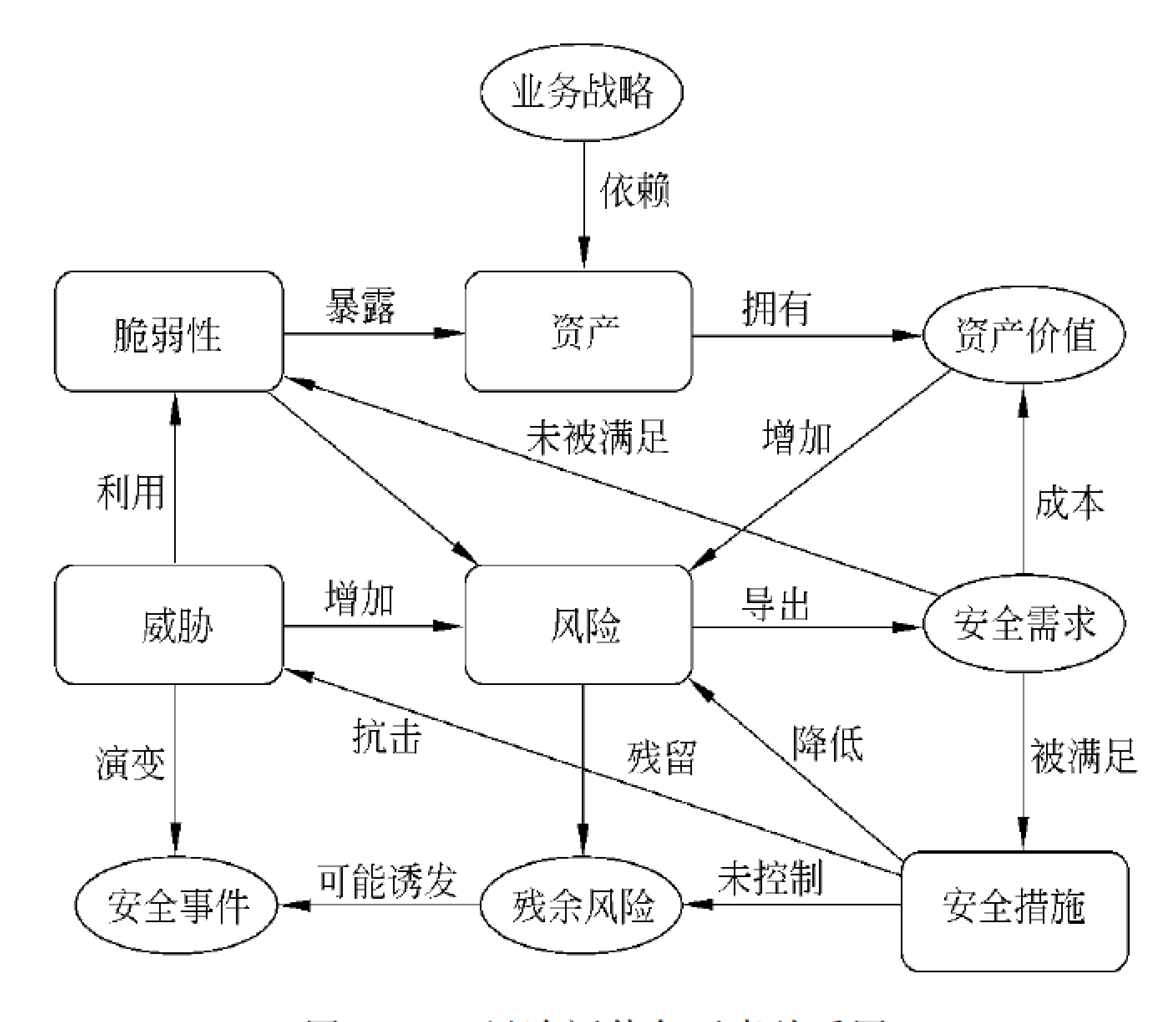


图 6-1-1 风险评估各要素关系图

一般地，进行风险评估可以按照以下五个步骤依次进行。

1. 资产识别与估价

为了明确被保护的信息资产，组织应列出与信息安全有关的资产，对每一项资产进行确认和适当的评估。为了防止资产被忽视或遗忘，在识别资产之前应确定风险评估范围。所有在评估范围之内的资产都应该被识别，因此要列出对组织的特定部门的业务过程有价值的任何事物，以便根据组织的商务流程来识别信息资产。在进行资产识别时，应考虑以下几方面：

(1) 数据与文档：数据库和数据文件、系统文件、用户手册、培训资料、运作和支持程序、持续性计划、应急安排。

(2) 书面文件：合同、方针、企业文件、保持重要商业结果的文件。

(3) 软件资产：应用软件、系统软件、开发工具和公用程序。

(4) 实物资产：计算机和通信设备、磁质媒体(磁带和磁盘)、其他的技术型设备(电源、空调)、家具、处所。

(5) 人员：具有特定技能的职员。

(6) 服务：计算和通信服务、其他的技术型服务(供热、照明、动力、空气)。

经过资产识别与估价后，组织应根据资产价值的大小进一步确定需要保护的关键资产。

2 威胁识别与评价

对组织需要保护的每一项关键信息资产进行威胁识别。在威胁识别过程中，应根据资产所处的环境条件和资产以前遭受威胁损害的判断，一项资产可能面临着多个威胁，同样一个威胁可能对不同的资产造成影响。威胁识别应确认威胁由谁或什么事物引发以及威胁评估的信息能够从信息安全管理的有关人员，以及相关商业过程中获得，这些人可能是人事部的职员、设备策划和IT专家，也包括组织内部负责安全的人员。

对威胁发生的可能性进行分析。确定威胁发生的可能性是风险评估的重要环节，组织应根据经验和(或)在关的统计数据来判断威胁发生的频率或者发生的概率。威胁发生的可能性受下列因素的影响。

资产的吸引力，资产转化成报酬的容易程度，威胁的技术含量，薄弱点被利用的难易程度。

威胁发生的可能性大小可以采取分级赋值的方法予以确定。例如，将可能性分为三个等级：非常可能=3；大概可能=2；不太可能=1。

威胁事件发生的可能性大小与威胁事件发生的条件是密切相关的。例如，消防管理好的部门发生火灾的可能性小。因此，上面根据经验或统计获得的威胁发生的可能性，可以是一个组织、相同或者社会的均值，对于具体环境的威胁发生的可能性应考虑具体资产的薄弱点予以修正：

$$PTV=PT\times PV$$

其中，PTV表示考虑资产脆弱性因素的威胁发生的可能性；PT表示未考虑资产脆弱性因素的威胁发生可能性；PV表示资产的脆弱性被威胁利用的可能性。

利用经过修正的威胁发生的可能性与威胁所产生的潜在影响两个因素可以测量风险。

评价威胁发生所造成的后果或潜在影响。威胁一旦发生会造成信息机密性、完整性

或可用性的损失,从而给组织造成不同程度的影响,严重的威胁发生会导致诸如信息系统崩溃、商务活动中断、财产损失甚至人身伤亡等重大安全事故。不同的威胁对同一资产或组织所产生的影响不同,即导致的价值的损失也不同,但损失的程度应以资产的相对价值(或重要度)为限。

威胁的潜在影响 I=资产相对价值 V×价值损失程度 CL

价值损失的程度 CL 是一个小于等于 1 大于 0 的系数,资产遭受安全事故后,其价值可能完全丧失(即 CL =1),但不可能对资产价值没有任何影响(即 CL≠0)。为简化评价过程,可以用资产的相对价值代替其所面临的威胁产生的影响。

3. 脆弱性识别与评价

由于组织缺乏充分的安全控制,组织需要保护的信息资产或系统存在着可能被威胁所利用的弱点,这些弱点可能来自组织结构、人员、管理、程序、资产本身的缺陷等。组织应针对每一项需要保护的信息资产,找出每一种威胁所能利用的脆弱性,并对脆弱性的进行评价。换句话说,就是对脆弱性被威胁利用的可能性 PV 进行评价,可以采用分级赋值的方法。

例如:非常可能=4,很可能=3,可能=2,不太可能=1,不可能=0。

4. 对已有的安全控制进行确认

组织应将已采取的控制措施进行识别并对控制措施的有效性进行确认,继续保持有效地安全控制,以避免不必要的工作和费用,防止控制的重复实施。对于那些确认为不适当的控制应核查是否应被取消,或者用更合适的控制代替。在风险评估之后选择的安全控制与现有的和计划的控制应保持一致。

安全控制可以分为预防性控制和保护性措施(如商务持续性计划、商业保险等),预防性措施可以降低威胁发生的可能性和减少安全脆弱性,而保护性措施可以减少因威胁发生所造成的影响。控制措施与风险程度的关系如图 6-1-2 所示。

5. 确定风险的大小与风险等级(即风险评估)

组织在经过资产识别与估价、威胁与脆弱性的识别与评价、已有控制措施的确认后,应利用适当的风险测量方法或工具确定风险的大小与风险等级,即对组织信息安全管理范围内的每一信息资产因遭受泄露、修改、不可用和破坏所带来的任何影响做出一个风险测量的列表,以便识别与选择适当和正确的安全控制方式,这也是组织策划信息安全管理体系的重要步骤。它具体包括以下三个子步骤:

1)风险测量方法——风险大小和等级评价原则

根据风险定义所知,风险是资产所受到的威胁、存在的脆弱性及威胁利用脆弱性所造

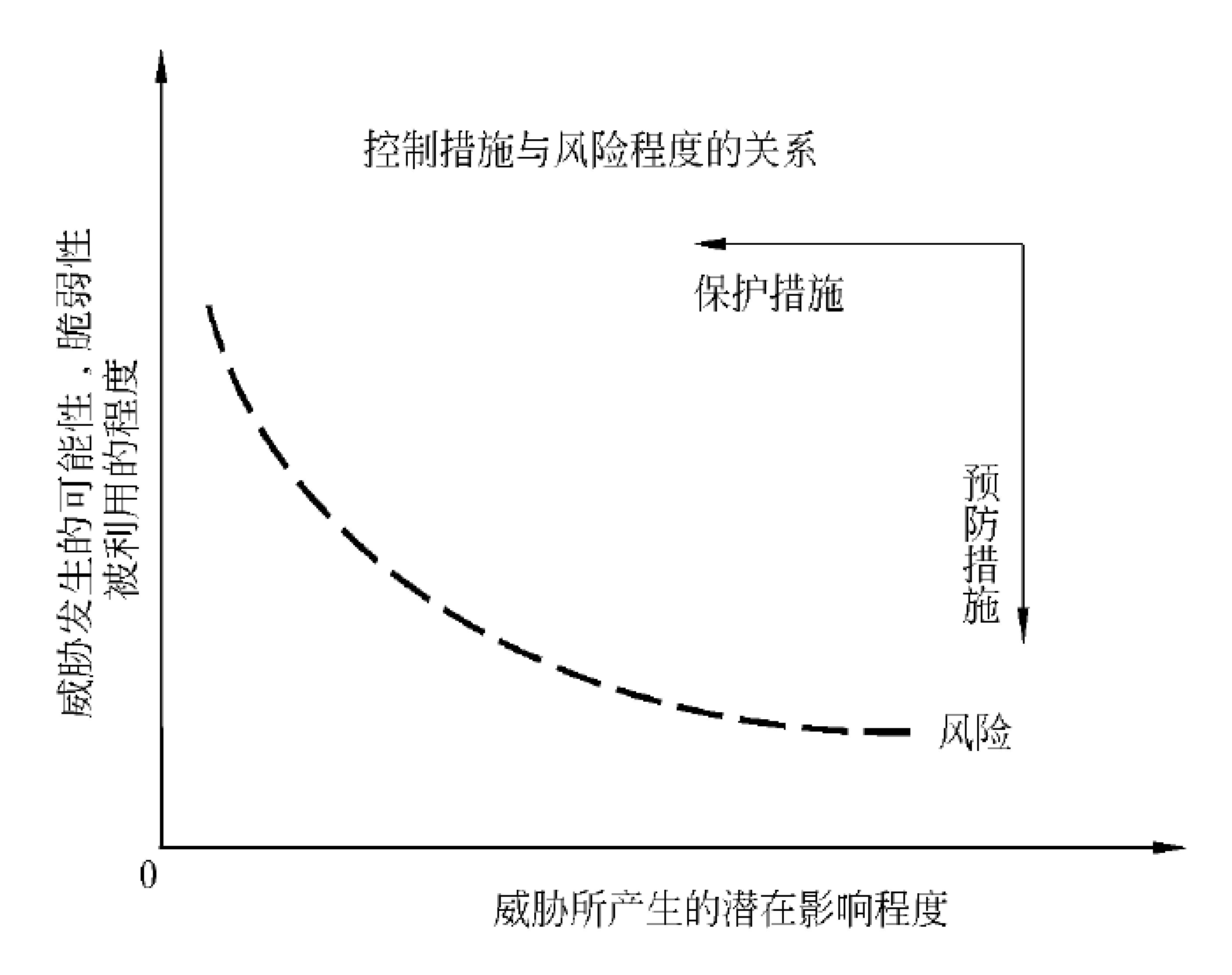


图 6-1-2 控制措施与风险程度的关系

成的潜在影响三方面共同作用的结果。风险是威胁发生的可能性(PT)、脆弱性被威胁利用的可能性(PV)和威胁的潜在影响(I)的函数，记为：

$$R=R(PT,PV,I)$$

其中，R 表示资产受到某一威胁所拥有的风险；RT 表示威胁发生的可能性；PV 表示脆弱性被利用的可能性；I 表示威胁的潜在影响，I=V×CL。

由于威胁的潜在影响 I 可以用资产的相对价值 V 来代替，上面的函数 R 可以改写为：

$$R=R(PT,PV,V)$$

以上两个公式都是考虑三个变量的风险计算函数。如果将威胁发生的可能性 RT 和脆弱性被利用的可能性 PV 综合为一个变量(因素)，即威胁真实发生的可能性(记为 PTV，PTV =PT×PV，其中，PT 可以被看做是威胁发生的平均可能性)，上述三元风险函数可以改写为如下的二元风险函数：

$$R=R(PTV,V)$$

无论二元还是三元风险函数，均为增函数，即风险随威胁的可能性、脆弱性的被利用的程度、资产的相对价值的增加(减少)而增加(减少)。资产的相对价值(V)与威胁真实发生的可能性(PTV)的关系如图 6-1-3 所示。

可以利用二元或三元的方法测量风险的大小。风险计算公式可以采用简单的乘法、矩阵风险表等方式表示。

风险评估有很多现成的工具可用。这些工具可以分成以下几类：

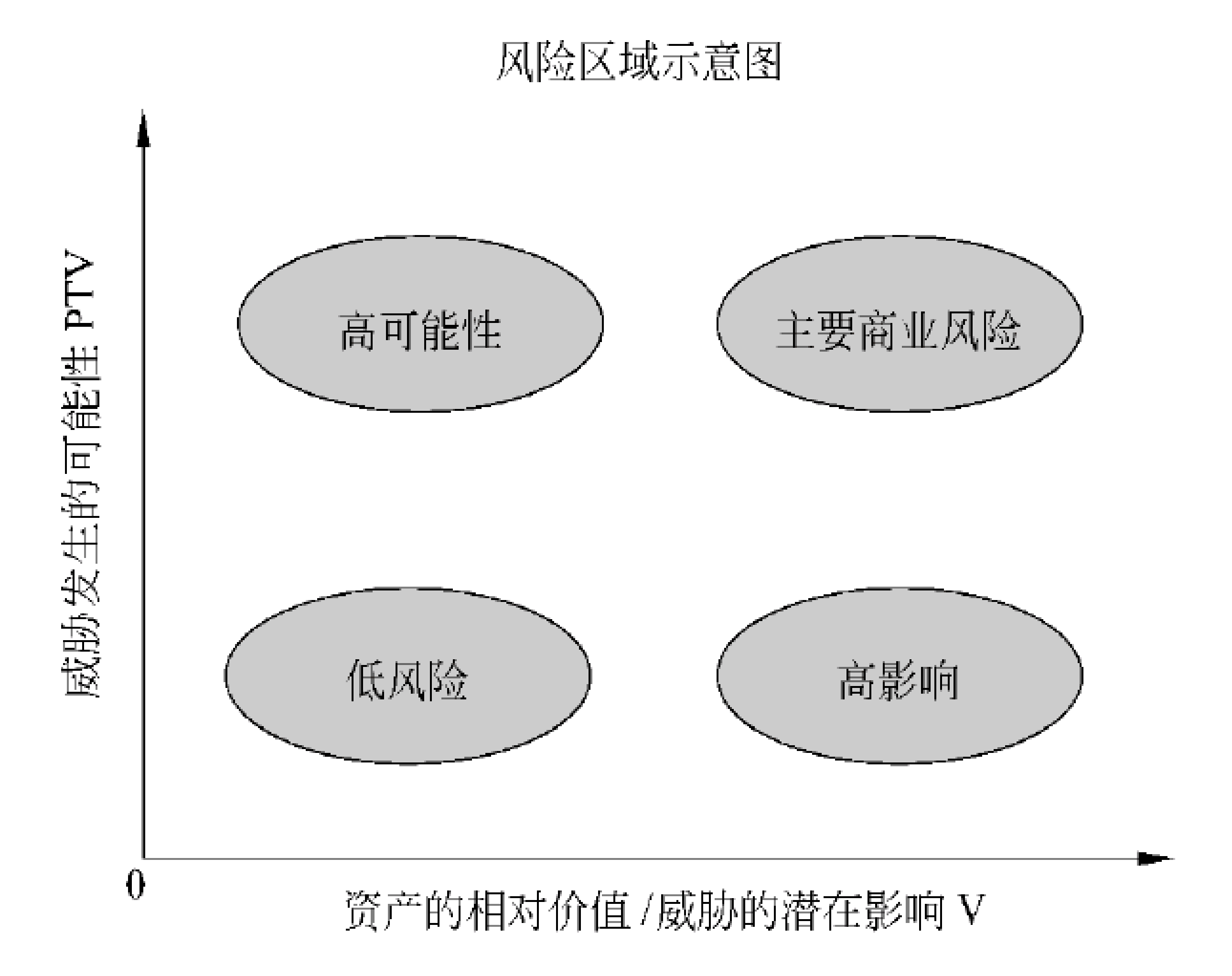


图 6-1-3　资产的相对价值(V)与威胁真实发生的可能性(PTV)的关系

(1) 扫描工具：包括主机扫描、网络扫描、数据库扫描，用于分析系统的常见漏洞。

(2) 入侵检测系统(IDS)：用于收集与统计威胁数据。

(3) 渗透性测试工具：黑客工具，用于人工渗透，评估系统的深层次漏洞。

(4) 主机安全性审计工具：用于分析主机系统配置的安全性。

(5) 安全管理评价系统：用于安全访谈，评价安全管理措施。

(6) 风险综合分析系统：在基础数据基础上，定量、综合分析系统的风险，并且提供分类统计、查询、TOP N 查询以及报表输出功能。

(7) 评估支撑环境工具：评估指标库、知识库、漏洞库、算法库、模型库。

无论采用哪一种风险测量方法或风险评估工具(无论是定性的还是定量的，是简单的还是复杂的)，要点都在于对威胁发生所造成的损失和威胁发生的可能进行量化，并且保证量化的结果对于负责风险决策的人是一致的和有意义的。需要特别说明的是，在进行风险评估时，绝不能因为使用了不同的风险测量方法或风险评估工具而形成不同的结论。

2) 确定风险的优先级别

确定风险数值的大小不是我们评估的最终目的，重要的是明确不同威胁对资产所产生的风险的相对值，即要确定不同风险的优先次序或等级，对于风险级别高的资产应被优先分配资源进行保护。组织可以采用按照风险数值排序的方法(机会损失成本)的平衡。

3) 选择风险评估——管理软件工具

在风险评估过程结束时，必须保存评估的结果(资产和它们的价值，威胁、脆弱性和风险等级等)，并进行相应的文件化处理(例如，将有关数据存储在数据库里)。

组织可以利用软件支持工具进行风险评估。这有助于简化再评估过程。

在选择与使用风险评估——管理软件工具时应该考虑以下事项。

(1) 最起码应该包括数据搜集、分析和结果输出模块。

(2) 所依据的方法应该反映组织的风险评估及管理的全部方法。

(3) 对风险评估和风险管理的结果能够方便的形成报告。

(4) 能够保持在数据搜集和分析阶段所采集信息的历史记录,以供将来的调查与评估。

(5) 必须有描述工具文件。

(6) 与组织中的硬件和软件协调并兼容。

(7) 考虑有关工具的使用培训。

(8) 有关工具的安装与使用指南。

但是,为了便于具体工作的顺利进行,人们更多的是采取如下 9 个步骤进行实际的风险评估。

① 体系特征描述;

② 识别威胁;

③ 识别脆弱性;

④ 分析安全措施;

⑤ 确定可能性;

⑥ 分析影响;

⑦ 确定风险;

⑧ 建议安全措施;

⑨ 记录结果。

各个步骤需要的输入和产生的输出表示在图 6-1-4 之中。

在实施风险评估的过程当中,有时首先根据不同级别的威胁对不同价值的资产可能形成的风险进行分级,进而选择适合级别的保证措施。这是一种安全需求提炼的过程。而对于计划和已经建设的系统,则应该考虑和分析测试系统可能存在的脆弱性。上述工作流程是一个大致应当遵循和不断重复循环的过程。但是在实践中,基于不同目的和条件,在不同阶段所进行的风险评估工作,也可简化或者充实其中的某些步骤。

6.1.3 有关标准

目前使用较多的信息安全评估标准如下:

(1) ISO/IEC 17799-1:2005 信息技术—信息安全管理实施细则(即 ISO/IEC 27002)。

(2) ISO/IEC 15408 IT 安全评估准则。

(3) ISO/IEC TR 13335:信息技术—安全技术—信息产业安全管理的指导方针。

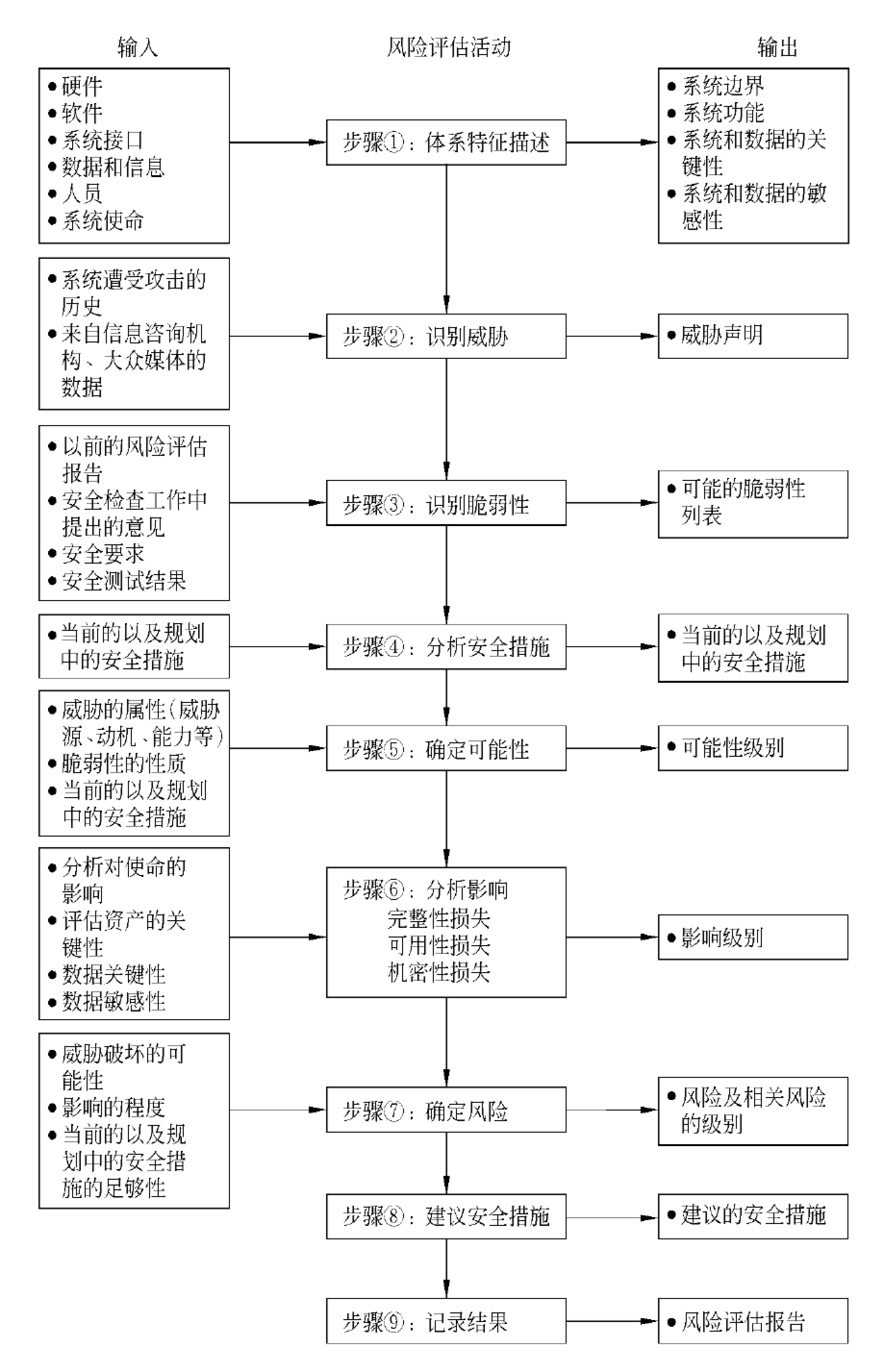


图 6-1-4　进行风险评估的实际工作流程

(4) GB/T 18336—2001：信息技术-安全技术-信息技术安全性评估准则。

(5) NSA：Systems Security Engineering Capability Maturity Model（简称 SSE-CMM）。

其中，有关 ISO/IEC 17799-1:2005 的内容在 6.2 节中介绍，有关 SSE-CMM 的内容在 7.1.1 节中说明，这里只简单介绍一下 ISO/IEC TR 13335。

ISO/IEC TR 13335 是由 ISO 组织和 IEC 联合出版的一份技术报告，由以下内容组成，各部分内容分别为：概括了信息技术安全方面的管理任务，提供安全概念和模型的介绍；用全面的观点来阐述信息技术安全的实施与管理；提供安全设施的选型指导，除了考虑安全问题和威胁之外，还需要考虑信息技术系统的类型；在介绍网络安全时，需要考虑对通信相关因素进行的鉴别和分析。

ISO/IEC TR 13335 这份标准包含了针对如何管理信息安全的全面指导。由于这份标准主要针对安全问题，因此并没有涵盖信息技术管理领域的所有职责。

与 ISO/IEC 17799-1:2005 相比，ISO/IEC TR 13335 只是一个技术报告和指导性文件，没有给出一个全面而完整的信息安全管理框架，相对而言更接近于一种指南，对具体环节切入较深，对实际工作给予了更多的指导价值，因而具有更好的可操作性。

6.2 信息安全管理标准 ISO/IEC 27002

6.2.1 背景

ISO/IEC 27002 的全称是“信息安全管理实践规则”，直接由 ISO/IEC 17799:2005 更改标准编号而来。

“ISO/IEC 17799-1:2005：信息技术-信息安全管理实施细则”是国际标准化组织（ISO）于 2005 年颁布的一项信息系统安全管理标准。目前，ISO/IEC 27002 已经在欧洲国家具有广泛的影响。

事实上，ISO/IEC 27002 起源于欧洲，其前身最早可追溯到英国于 1993 年发布的 BS 7799（发展历程见图 6-2-1）。这是当年由英国贸易工业部（DTI）立项，并在 BSI/DISC 的 BDD/2 信息安全管理委员会的指导下制定完成和向外发布了最初的版本。

随后，英国于 1995 年首次正式出版了 BS 7799-1:1995《信息安全管理实施细则》。该细则提供了一套综合的、由信息安全最佳惯例组成的实施规则，目的是确定能够适用于大、中、小型工商业信息系统在大多数情况下所需控制范围的唯一参考基准。

1998 年，英国又公布了 BS 7799-2:1998《信息安全管理体系规范》。作为 BS 7799-1

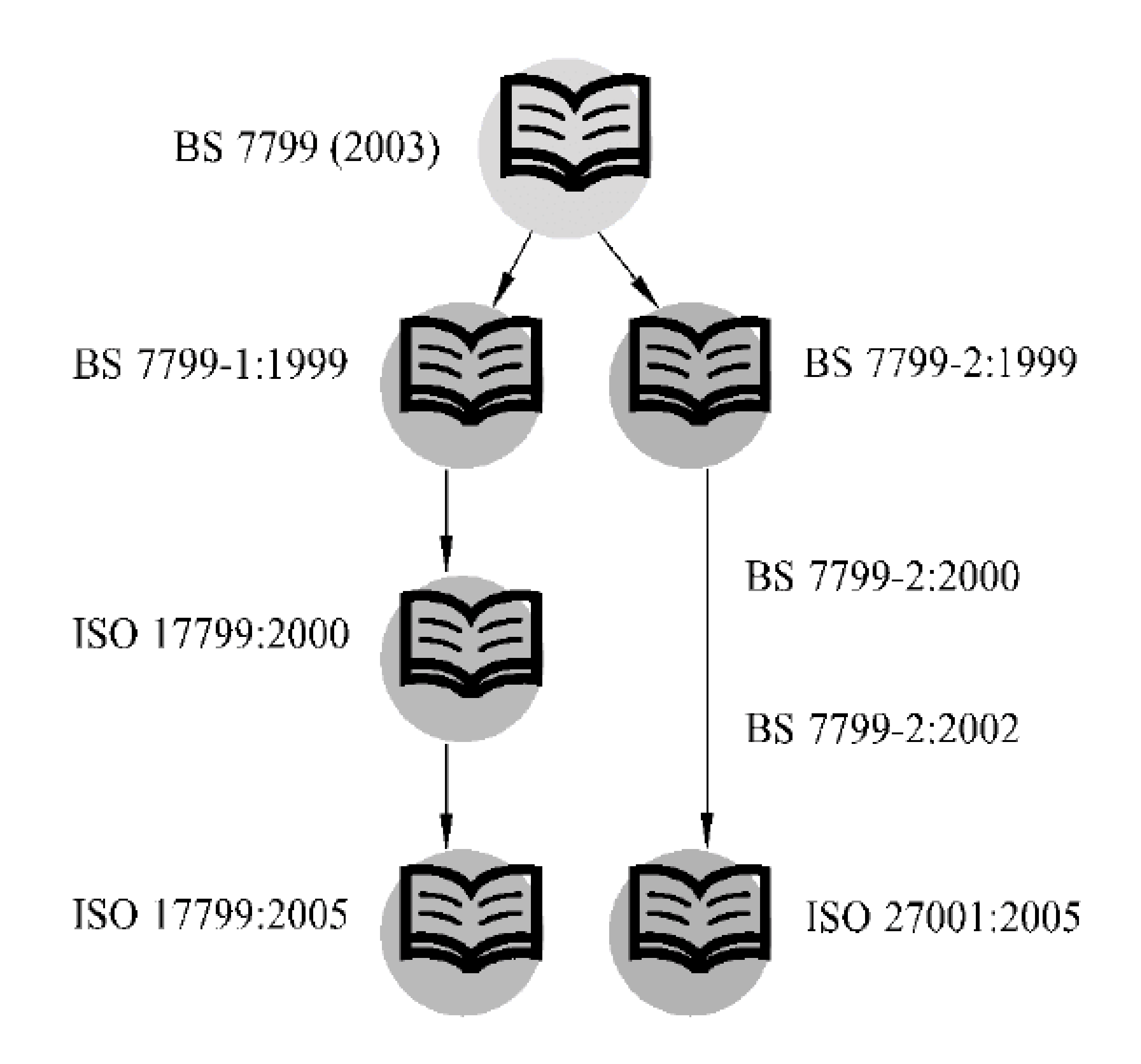


图 6-2-1　BS 7799 标准发展历程

的补充部分，BS 7799-2 规定了信息安全管理体系要求和信息安全控制要求，可以用于针对一个具体组织的全面或部分信息安全管理体系进行评估活动。因此，BS 7799-2 自出现之初便被认为可以作为一个正式认证方案的依据。

1999 年，BS 7799-1 和 BS 7799-2 经过修订得以重新发布，即 BS 7799-1：1999《信息安全管理实施细则》和 BS 7799-2：1999《信息安全管理体系规范》。新版本考虑了信息处理技术（尤其是网络和通信领域当时的最新发展状况），同时还特别强调了商务涉及的信息安全和信息安全的责任。

其中，BS 7799-1：1999 主要为组织制定其信息安全标准和进行有效地信息安全控制提供一个大众化的最佳惯例，推进企业间的贸易往来，尤其是为使用电子商务的企业的共享信息的安全问题提供信任。

BS 7799-2：1999 规定了建立、实施信息安全管理体系（ISMS）并对其进行归档的要求，以及依据组织的需要来实施安全控制的要求，主要用于一个组织进行有效地风险管理和寻求信息安全管理体系第三方认证标准这两种情况。BS 7799-2：1999 标准分为两类，即信息安全管理体系要求和信息安全控制要求。它在管理思想上遵循 PDCA 模型中提出的持续改进的管理模式。

2000 年 12 月，BS 7799-1：1999《信息安全管理实施细则》被国际标准化组织 ISO 接纳并正式成为国际标准，其全称是：ISO/IEC 17799-1：2000《信息技术——信息安全管理实施细则》。

此后，ISO/IEC 17799-1：2000 继续得以应用和改进。2005 年 10 月，ISO 在广泛吸纳

了业界的最新发展成果和听取各方建议的情况下，发布了该标准的修订版，即 ISO/IEC 17799-1:2005《信息技术——信息安全管理实施细则》，使之作为信息安全管理的国际标准，更加适合为全球范围内成千上万家正处于成长阶段的电子商务团体提供服务。它强调尽最大可能地保证信息的安全，提供商务最佳惯例、指南以及在任何组织实施、维护、管理信息安全，和以任何形式生产和使用信息的一般原则。

ISO/IEC 17799:2005 认识到纯粹以技术手段实现信息安全管理的效果将非常有限。评定一个组织所需要的安全级别必须依赖合适的管理控制手段和程序，通过评估风险级别及相关因素来确定进行信息安全管理的合理投入。信息安全管理工作需要组织的所有员工主动参与，有时还需要股东、供应商、第三方和客户的积极参与。

ISO/IEC 17799:2005 还确定了进行信息安全管理必须从源头上给以关注的思想。这些源头包括关键的成功要素，具体是：从事信息安全管理工作的组织结构，资产管理状况，人力资源状况，物理和环境安全状况，通信和操作管理状况，信息系统采办，研制和维护状况，突发事件管理状况，业务连续性管理状况，以及对于有关法律法规的遵从与否。

ISO/IEC 17799:2005 标准编制组的组长泰德·汉姆弗雷对修订版进行了非常客观、准确的评价。他说："该修订版标准为各组织提供许多以前没有的、经改进的信息安全管理的最佳实施惯例。例如，它帮助这些组织更好地管理外部业务、外部采办和服务提供商的保密安全事务；增强事件处理能力；处理 patch 管理、移动设备、无线技术和通过互联网传播的有害手机代码等问题；同时，它还改进了人力资源管理的最佳惯例，并具有其他几个新亮点"。此外，泰德·汉姆弗雷还表示："该标准的使用者还可以向其业务伙伴、客户和供应商展示其信息的安全机密性，从而将其在信息安全管理方面的投资转化为真正的商业机会，在激烈的行业竞争中获得竞争优势"。

2007 年 4 月 ISO/IEC 17799:2005 更改编号为 ISO/IEC 27002，成为 ISO/IEC 27000 系列标准中的一员。

在 ISO/IEC 17799:2000 得以修订和改进的同时，BS 7799—2:1999 也获得了 ISO 的进一步关注。2005 年 11 月，ISO 在 BS 7799-2:1999 的基础上正式发布了 ISO/IEC 27001《信息安全管理系统要求》。与 ISO/IEC 17799:2005 不同的是，ISO/IEC 17799:2005 虽然是信息安全管理标准，但其设计初衷不是为了支持认证，因而也不适用于认证工作，而 ISO/IEC 27001 恰好主要用于认证领域。

总而言之，ISO/IEC 17799/BS7799 提供了一个开发组织的信息安全标准，以及有效实施安全管理的公共基础，同时还在一定程度上确保了不同的组织之间进行交易所需的可信度，符合信息安全"七分管理，三分技术"的原则。组织可以按照该标准建立完整的信息安全管理体系，并且通过实施和保持该体系，达到动态的、系统的、全员参与的、制度化的、以预防为主的信息安全管理方式，用最低的成本获得可接收的信息安全水平，保证组织的业务连续性。

6.2.2 主要内容

ISO/IEC 27002 标准有 11 个控制项、39 个控制目标、133 个控制措施。其中,11 个控制项分别是:

(1) 信息安全方针(Security policy)。

(2) 组织信息安全(Organization of information security)。

(3) 资产管理(Asset management)。

(4) 人力资源安全(Human resources security)。

(5) 物理和环境安全(Physical and environmental security)。

(6) 通信和操作管理(Communication and operation management)。

(7) 访问控制(Access control)。

(8) 信息系统的获取、开发和维护(Information systems acquisition, development and maintenance)。

(9) 信息安全事故管理(Information security incident management)。

(10) 业务连续性管理(Business continuity management)。

(11) 符合性(Compliance)。

各控制项的详细内容可参见表 6-2-1。

该标准由以下两个部分组成。

(1) 信息系统安全管理业务守则:为信息系统安全提供了一套全面综合了最佳实践经验的控制措施,目的是在信息系统被用于工业和商业用途时,为确定实施控制措施的范围提供一个可供不同规模的组织采用的参考依据。“业务守则”部分的内容详细而且系统,具体包括:安全策略;安全组织;资产分类与控制;人员安全;物理与环境安全;通信与操作管理;访问控制;系统开发与维护;业务连续性管理;遵循性等。

(2) 信息系统安全管理系统规范:提供了各种组织构建信息系统安全管理系统的途径和方式,提供了用于建立该标准的信息系统安全管理系统的指导框架,指出了构建信息系统安全管理系统的基本步骤和方法,定义了一个信息系统安全管理系统的主要构成文档。

需要强调指出的是,ISO/IEC 17799 不是一篇技术性的信息安全操作手册,作为一个通用的信息安全管理指南,其目的并不是说明有关“怎么做”的细节,它所阐述的主题是安全策略和优秀的、具有普遍意义的安全操作。该标准特别声明,它是“制定一个机构自己的标准的出发点”,并不是说它所包含的所有方针和策略都是放之四海而皆准的。作为对各类信息安全问题的高级别概述,ISO/IEC 17799 有助于人们在高级管理中理解每一类信息安全主题的基础性问题。它广泛涵盖了几乎所有的安全议题,主要告诉管理者关于安全管理的注意事项和安全制度,这些规定一般单位都可执行。因此,需要建立信息安全

管理体系的单位可以此为参照，建立自己在这方面的体系，并在别人经验的基础上根据自身情况进行设计、取舍，以达到对信息进行良好管理的目的。

表 6-2-1 ISO/IEC 27002 内容一览表

章节序号	章节名称	内容说明	控制目标数量	控制措施数量
5	信息安全方针	建议组织应有一个阐明信息安全方面的宗旨和方向的信息安全方针，并形成方针文件，还应对这个方针文件进行定期评审	1	2
6	组织信息安全	这里的“组织”，兼有动词和名词两层意思。组织的信息安全工作应建立一个管理框架，即组织机构，以确定信息安全工作的领导、工作落实、内部外部协调与合作、职责分配等。在这一章节中，还提出了第三方服务和外包活动中的信息安全控制	2	11
7	资产管理	“资产”是这个标准中的一个重要概念。标准在引言中开宗名义：“信息是一种资产，像其他业务资产一样，对组织具有价值”。“资产”是信息安全工作主要的保护对象。信息安全就要首先知道保护什么，然后考虑保护到什么程度，再决定怎样保护	2	5
8	人力资源安全	“人”在信息安全活动中既是主体，也是客体。主体是指许多信息安全控制措施的实现是由“人”来完成；客体是指“人”也是信息安全活动中要保护的对象。经验告诉我们，一个组织重要的、有价值的信息大多数存在于员工的大脑中，许多信息安全事件的发生是由人而起。“人”在信息安全活动中也是最复杂、最难控制的保护对象。在这个章节中，标准提供了与“人”有关的 3 个控制目标和 9 个控制措施	3	9
9	物理和环境安全	物理和环境的安全控制不仅是信息安全的需要，也是传统安全的要求。一个组织无论是否考虑信息安全问题，都要把物理和环境安全做好。因此，本章节介绍的这些目标和控制措施是最容易理解、最容易实施的	2	13
10	通信和操作管理	“通信”是广义的概念，主要指信息交换、沟通和交流等活动。操作主要指对信息处理设备和设施、信息系统、软件等的操作	10	32
11	访问控制	访问控制是保持信息机密性的必要措施，这一章从访问控制策略、用户访问管理、网络访问、操作系统访问、应用系统访问、访问和使用监督、移动计算和远程工作等方面提出了 7 个控制目标和 25 项控制措施	7	25

续表

章节序号	章节名称	内容说明	控制目标数量	控制措施数量
12	信息系统的获取、开发和维护	主要从应用系统的开发建设和运行维护的过程中与信息安全有关的方面提出了详细的控制目标和控制措施,还提到了与密码相关的控制措施	6	16
13	信息安全事故管理	目前,还没有一项信息安全控制措施是一劳永逸的。无论你制定和实施怎样的信息安全风险处理计划,信息安全事件总有可能发生。对信息安全事件的正确管理是重要的	2	5
14	业务连续性管理	业务连续性管理(BCM)是目前的热门话题,并逐渐成为一门专业。对企业来说,BCM 是一项重要的、综合的管理,涉及企业的诸多方面,信息安全问题应该是其中的一个方面	1	5
15	符合性	满足我国当前适用的法律法规中关于信息安全方面的要求,是任何组织首先要做的;其次是满足合同要求、组织制定的规章制度和技术要求等。本章所提出的控制目标和控制措施,就是为了控制这些方面的信息安全风险	3	10
合计			39	133

6.2.3　应用情况

现在,ISO/IEC 27002 已经成为国际上具有代表性的信息安全管理体系标准。欧美发达国家(例如英国、荷兰、丹麦、澳大利亚、巴西)和部分亚洲国家或地区(如日本、新加坡、韩国、中国香港、中国台湾)的政府机构、银行、证券、电信行业等机构、组织和企业都已经采用该标准进行信息安全管理。

这些应用主要体现在以下四方面:

(1) 具有强烈信息系统安全需求的组织(尤其是政府部门、银行、电信、保险和 IT 企业)纷纷参照该标准建立各自的信息系统安全管理系统。

(2) 许多国家的政府部门(例如,中央银行、银行同业协会等金融监管当局)利用该标准构建自己的信息系统安全监管准则。

(3) 英国标准协会等标准化组织正积极推动安全管理标准的认证工作。

(4) 众多信息系统安全技术公司遵循该标准推出安全产品和安全服务。

由于该标准所体现的信息与信息系统安全理念具有充分的合理性并且具有较强的操作性,它对于许多机构、组织和企业建立信息系统安全和技术风险监管体系都具有广泛而

且重要的指导意义。

6.3 信息安全等级保护

6.3.1 国外信息安全等级保护

信息安全等级保护与信息系统安全保护密切相关。信息系统安全保护是通过保护信息系统本身的安全,达到保护信息系统中信息安全的目的。信息系统安全的内涵是实现系统正常运行,保障信息的完整性、可用性、机密性、不可否认性和可控性。其中,机密性、完整性、可用性是基本安全特性要求。信息系统安全的外延表现为部门职能和业务的正常运转。

当前,各国都在从国家安全发展战略出发,考虑和加强信息系统安全保护工作,把涉及国计民生的信息系统作为重点保护对象。但是,不同的国家对于重点信息系统的概念略有不同。例如,美国称这些系统为"关键信息基础设施",而我国称这些系统为"重要领域的信息系统"。

在网络互联互通的情况下,国家信息系统安全问题的实质是国家主权、政治、经济、国防、社会安全。因此,各国在信息系统安全保护方面的主要思路和对策基本相同,即都注重加强关键信息基础设施安全保护,提高整体防护水平,强化政府监管力度。

以美国为例,它在这方面的主要工作包括:1998 年 5 月 22 日,颁布了《保护美国关键基础设施》的总统令,相继又制定了《信息保障技术框架》,成立了相关的信息安全组织机构,明确制定了新的国家信息网络安全战略、合理的信息安全战略发展目标和任务、重点保护国家关键信息基础设施的安全;同时有计划、有步骤地发展网络攻击和反攻击技术;完善国家网络安全监管体系;提高网络安全技术水平;建立网络安全防护体系。为此,主要采取以下措施:在实行等级保护标准的基础上,进一步完善等级保护程序,严格控制对政府信息资源访问;加强信息发布审查及控制机制,清理政府网站上的有害信息等;开发网络预警系统,加强网络自身防护和生存能力;提高网络的攻击能力,完善信息安全法律体系等。

6.3.2 我国信息安全等级保护

在我国,"信息安全等级保护"指的是:对涉及国计民生的基础信息网络和重要信息系统按其重要程度及实际安全需求,合理投入,分级进行保护,分类指导,分阶段实施,保障信息系统安全正常运行和信息安全,提高信息安全综合防护能力,保障国家安全,维护

社会秩序和稳定，保障并促进信息化建设健康发展，拉动信息安全和基础信息科学技术发展与产业化，进而牵动经济发展，提高综合国力。

实行信息安全等级保护主要是为了确保信息安全保护符合客观存在和发展规律。信息系统是应社会发展、社会生活和工作的需要而设计和建立的，是社会构成、行政组织体系的反映，由于这种体系是分层次和级别的，与其对应的各种信息系统在社会和经济价值方面也具有不同的等级，并客观上体现为系统基础资源和信息资源的价值大小、用户访问权限的大小、大系统中各子系统重要程度的区别等表现因素。信息安全保护分级、分区域、分类、分阶段是做好国家信息安全保护必须遵循的客观规律。

我国政府非常重视信息安全等级保护工作。早期与之相关的一系列工作主要有：

(1) 1994 年 2 月 18 日，国务院颁布了《中华人民共和国计算机信息系统安全保护条例》，以国家法律的形式规定“重点保护国家事务、国家经济建设、国防建设、国内尖端科学技术等重要领域的信息系统的安全。”同时规定“计算机信息系统实行安全等级保护，安全等级的划分标准和安全等级保护的具体办法，由公安部会同有关部门制定。”这些重要领域的信息系统也就是涉及国计民生的国家关键信息基础设施，包括国家互联网。其中国家事务信息系统涵盖国家电子政务信息系统。这些法律制度的规定具有十分重要的战略意义。

(2) 1998 年 12 月，公安部与国家密码管理委员会、信息产业部、国家保密局等相关部门就当前国家信息化建设中的安全策略和安全技术、安全等级保护制度基础建设等问题进行了深入研究，并在充分征求和吸收各方意见的基础上，起草了《计算机信息系统安全保护等级制度建设纲要》，确立了安全保护等级制度的主要适用范围、建设目标、建设原则、建设任务、实施步骤及措施等主要问题。

(3) 1999 年 9 月 13 日经国家质量技术监督局审查通过并正式发布了强制性国标《计算机信息系统安全保护等级划分准则》GB 17859—1999，将信息系统划分为五个安全保护等级：用户自主保护级、系统审计保护级、安全标记保护级、结构化保护级和访问验证保护级。安全保护能力从第一级到第五级逐级增强。GB 17859—1999 的发布实施，表明我国信息系统安全保护实行五级保护。但是，GB 17859—1999 的有效贯彻实施，还需要由相应的管理办法及配套标准体系、等级产品及系统检测评估工具、测评机制等，构成完整的安全等级保护体系。

(4) 2000 年 11 月 10 日，国家计委下达了由公安部主持开展的《计算机信息系统安全保护等级评估认证体系及互联网络电子身份认证管理与安全保护平台试点》项目建设的任务(以下简称“1110 工程”)。“1110 工程”的总体建设目标是：建立我国信息系统安全等级保护监督管理和网络身份认证管理服务体系，为加强对重要领域信息系统和互联网的安全监督管理提供必需条件。“1110 工程”的主要内容：以信息系统的安全监督管理

为核心,初步建立信息系统安全等级保护监管体系。2003 年初,“1110 工程”中的主要项目取得了以下成果:

① 依据《中华人民共和国计算机信息系统安全保护条例》和《计算机信息系统安全保护等级划分准则》组织起草了《信息系统安全保护等级管理办法》草案,重点就信息安全保护制度化、等级化、规范化,法制化建设,研究提出了从总体上把握国家信息安全保护关键环节,建立长效安全保护机制的整体思路和办法。

② 为了实现我国信息系统安全的整体化、规范化保护,以工程带标准的办法,制定并发布了一批“1110 工程”项目成果应用推广所需的重要标准,并提出了比较完整的安全保护标准体系,分三批完成发布,其中包括:《计算机信息系统安全保护等级通用技术要求》、《计算机信息系统网络安全保护等级技术要求》、《计算机信息系统操作系统安全保护等级技术要求》、《计算机信息系统数据库管理系统安全保护等级技术要求》、《计算机信息系统安全保护等级管理要求》等。

③ 安全保护等级评估工具(包括 2 套系统评估工具和 9 套产品评估工具)。

④ 基本完成上海安全产品等级检测中心建设,北京信息系统安全保护等级评估中心正在加紧筹建。

⑤ “郑州粮食交易市场网络电子身份认证示范工程”(电子商务环境下的身份认证)和“南海市网络电子身份认证示范工程”(电子政务环境下的身份认证)。

⑥ 在国家计委项目——网络身份认证管理示范工程的基础上,逐步开展了以公安户政信息和特征识别码为支持平台的网络身份管理工作。

这些成果为全面开展信息系统安全等级保护制度建设奠定了比较坚实的基础,为随后的等级保护试点工作和全国范围的等级保护推广工作提供了经验。

近几年,公安部联合其他一些国家机构以《信息安全等级保护管理办法》为核心进行了一系列研究、尝试、试点工作。正式的《信息安全等级保护管理办法》已于 2007 年 6 月 22 日,由公安部、国家保密局、国家密码管理局、国务院信息化工作办公室等国家四部委制定完成并审批通过,并自发布之日起施行。2006 年 3 月 1 日起施行的《信息安全等级保护管理办法(试行)》(公通字[2006]7 号)同时废止。

6.3.3 国家信息安全等级保护制度

经党中央和国务院批准,国家信息化领导小组已经决定加强信息安全保障工作,实行信息安全等级保护,重点保护基础信息网络和重要信息系统安全,抓紧安全等级保护制度建设。该决定明确落实了《中华人民共和国计算机信息系统安全保护条例》中关于实行信息安全等级保护制度的有关规定,提出了从整体上根本上解决国家信息安全问题的办法,进一步确定了我国信息安全的发展主线、中心任务,提出了总要求。对信息系统实行等级

保护是国家法定制度和基本国策，是开展信息安全保护工作的有效办法，同时也是信息安全保护工作的发展方向。实行信息安全等级保护的决定具有重大的现实意义和战略意义。

实行信息安全等级保护制度的目的是统一信息安全保护工作，推进规范化、法制化建设，保障安全，促进发展。

实施等级保护的必要性在于等级保护是信息系统的社会价值和经济价值保护的客观要求，即按信息的敏感和重要程度、系统应用性质和资产价值、部门重要程度，分级采取科学、合理的保护措施；对于涉及国计民生的国家关键信息基础设施应分级加以重点保护；适度保护，效费合理，避免盲目和浪费；对信息系统实行等级保护是国家法定制度。

国家实行信息安全等级保护制度，有利于建立长效机制，保证安全保护工作稳固、持久地进行下去；有利于在信息化建设过程中同步建设信息安全设施，保障信息安全与信息化建设相协调；有利于突出重点，加强对涉及国家安全、经济命脉、社会稳定的基础信息网络和重要信息系统的安全保护和管理监督；有利于明确国家、企业、个人的安全责任，强化政府监管职能，共同落实各项安全建设和安全管理措施；有利于提高安全保护的科学性、针对性，推动网络安全服务机制的建立和完善；有利于采取系统、规范、经济有效、科学的管理和技术保障措施，提高整体安全保护水平，保障信息系统安全正常运行，保障信息安全，进而保障各行业、部门和单位的职能与业务安全、高速、高效地运转；有利于信息安全保护科学技术和产业化发展。

信息安全等级保护要贯彻突出重点、兼顾一般的原则。等级保护制度要求落实各级安全责任。国家重点保护下列基础信息网络和重要信息系统：

(1) 国家事务处理信息系统(党政机关办公系统)。

(2) 金融、税务、工商、海关、能源、交通运输、社会保障、教育等基础设施的信息系统。

(3) 国防工业、国家科研等单位的信息系统。

(4) 公用通信、广播电视传输等基础信息网络中的计算机信息系统。

(5) 互联网网络管理中心、关键结点、重要网站以及重要应用系统。

(6) 其他领域的重要信息系统。

国家实行信息系统安全等级保护的形式是：国家意志、政府行为、科研单位、企业、社会广泛参与。

其中，“国家意志”指的是国家必须有统一的信息系统安全保护的法律规范、技术规范。

“政府行为”指的是：在国家信息化领导小组的统一领导，在国务院信息化工作办公室的统一组织、协调下，各级政府及其内部各部门应当对其信息系统安全建设与管理负责，开展信息系统安全等级保护工作。首先，各级政府在信息化建设过程中，应该按照等

级保护政策法规规定、管理与技术规范，组织进行信息系统安全等级保护建设、管理。其次，信息安全保护职能部门要严格依法行政，履行职责，做好安全等级保护工作。法律、法规和标准确定之后，政府信息安全保护职能部门的监督管理是推进和保障信息安全保护的关键。如果没有有效贯彻推进措施，再好的法律和标准也发挥不了其应有的效力。第三，信息系统安全涉及社会的方方面面，有关科研机构和企业应积极开发市场所需等级保护安全技术和产品。全社会要提高信息安全保护意识，职业道德，自觉遵守有关法律、法规，创造和维护良好的信息安全保护社会环境。

等级保护的工作程序是：

(1) 使用单位应该按照其处理信息的敏感程度、业务应用性质和部门重要程度是不同的，根据标准和有关规定确定其信息系统的安全保护等级，选择符合该安全保护等级要求的安全专用产品，安全建设和管理信息系统。

(2) 生产信息系统安全专用产品的企业在研制、生产等方面应当符合国家有关安全保护等级标准，并由通过行政机关认可的机构对其产品进行评测。

(3) 行政机关依据信息系统安全保护等级的管理办法和标准，对信息系统安全保护等级工作进行监督管理。

目前，各地区已经开始依据《信息安全等级保护管理办法》(公通字[2007]43 号)和《信息安全技术信息系统安全等级保护定级指南》，开始了系统安全保护等级划分和网络和信息系统定级备案工作，后续的信息系统建设、整改、测评等工作也将按步骤进行。

6.3.4 国家信息安全等级保护的有关标准

标准化建设在信息安全等级建设中占据着重要作用。实施信息安全等级保护制度必须遵循一定的标准。目前，国家已经建立了一套相对完善的信息安全等级保护标准，包括：基础性标准、构建过程控制标准、评测过程控制标准和运行过程控制标准。

其中，基础性标准包括：

(1) GB 17859—1999 计算机信息系统安全保护等级划分准则，这是其他标准的基础。

(2) 信息系统安全等级保护实施指南，为等级保护的实施提供指导。

构建过程控制标准包括：

(1) 技术要求标准。

(2) 产品要求标准。

测评过程控制标准包括：

(1) 系统测试与评估标准。

(2) 产品测试域评估标准。

运行过程控制标准包括：

(1) 工程管理标准,为管理工程实施提供指导。

(2) 系统管理标准,对系统运行过程的管理提供指导。

(3) 监督、检查管理标准,为按等级保护要求对信息系统的构建、测评、运行过程进行监督、检查、管理提供指导。

上述标准构成了一个标准体系。

该体系的基本思想是:以信息安全的五个属性为基本内容,从实现信息安全的五个层面,按照信息安全五个等级的不同要求,分别对安全信息系统的构建过程、测评过程和运行过程进行控制和管理,实现对不同信息类别按不同要求进行分等级安全保护的总体目标。

该体系的特点是:

(1) 完备性:对信息安全的五个属性,从五个层面、按五个等级确定安全功能要求和安全保证要求;对安全系统的构建、测评、运行三个过程进行全面控制。

(2) 整体保护性:实现信息的机密性、完整性和可用性(包括抗否认性、可控性和可操作性等),以及系统安全运行控制。

(3) 技术先进性:标准体系是在充分了解国际上当前信息安全技术及其标准发展的基础上,汲取先进的安全技术确定,并与国际接轨。

(4) 实用性:充分考虑到我国信息技术的发展和信息安全的现状,从制定可行的信息系统安全方案出发,适用于我国信息安全等级管理的需要。

(5) 前瞻性和可扩展性:标准体系所确定的技术和管理,具有一定的前瞻性,并可根据信息安全技术的发展改进和扩展。

(6) 具有充分的法律依据和执法保证:147 号令、27 号文件明确规定我国信息安全实施等级保护;执行过程控制标准适用于安全等级管理对安全系统及安全产品从设计、实现、检测、评估到监督、检查的管理需要;有相应的执法人员(如电子警察)确保等级保护的贯彻执行。

6.4　信息安全管理体系

6.4.1　背景

信息安全管理体系的思想源于 ISO 9000《质量管理体系》和英国标准学会(BSI)的 BS 7799-2。

国际标准化组织 1987 年发布了世界上第一个质量管理和质量保证系列国际标

准——ISO 9000 系列标准。20 年来,该标准推动世界各国工业企业的质量管理和供需双方的质量保证,促进国际贸易交往起到了很好的作用。ISO/TC176 分别在 1994 年和 2000 年对 ISO 9000 质量管理标准进行了两次全面的修订。由于该标准吸收了国际上先进的质量管理理念,采用了 PDCA 循环的质量哲学思想(规划——Plan,实施——Do,检查——Check,处置——Act),给出了一个科学的、逻辑性强的体系,采用与具体产品的技术无关的过程管理的思想,对于产品和服务的供需双方都具有很强的实践性和指导性。PDCA 模型如图 6-4-1 所示。

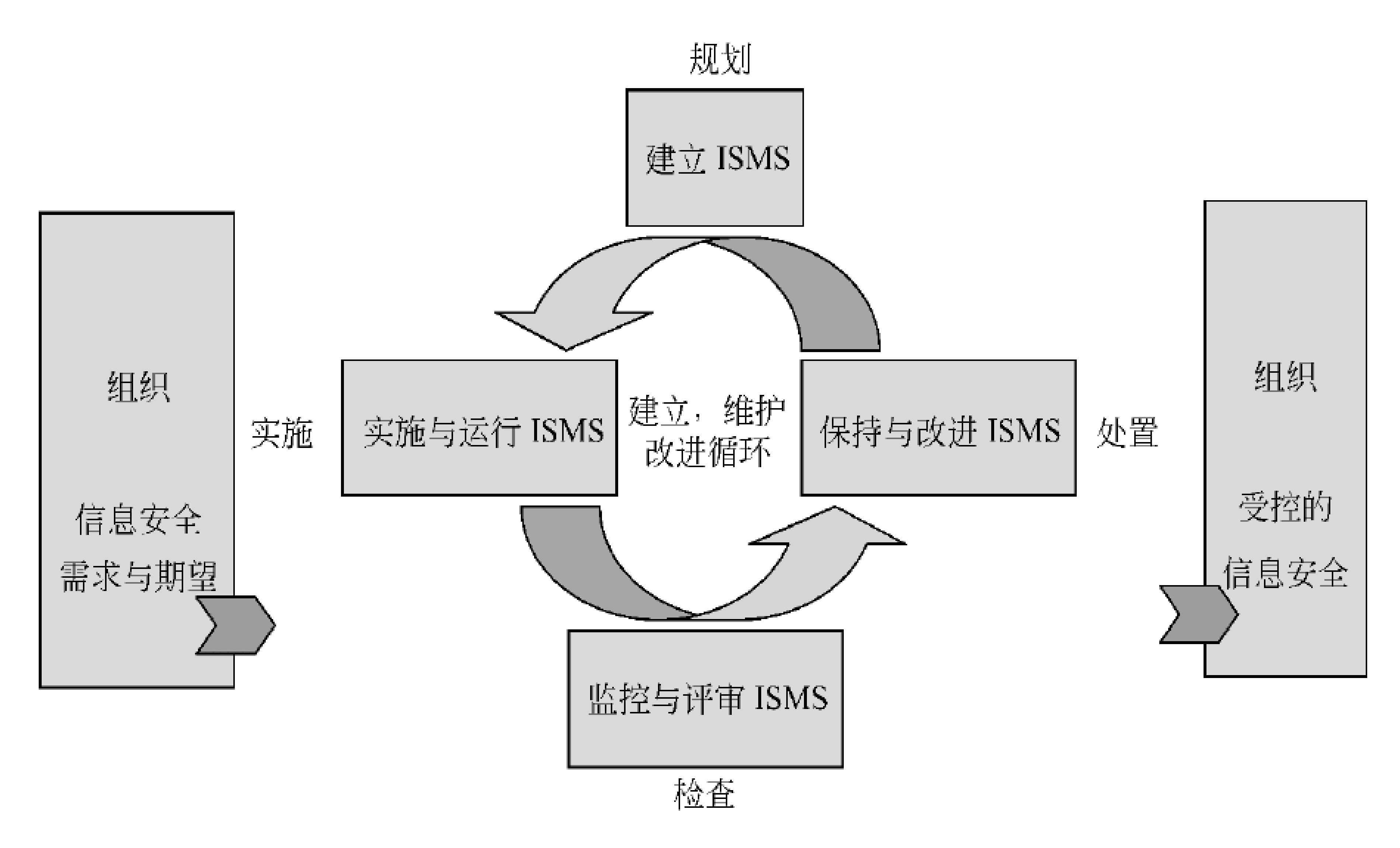


图 6-4-1　PDCA 模型

在 ISMS 的规划设计阶段,就要求从定义 ISMS 的执行范围和政策出发,执行风险评估,对风险评估处理做出决定最后落实到安全控制措施的选择上。

在 ISMS 的建立阶段,需要做以下事情:

(1) 根据组织及其业务特点、位置、资产、信息体系边界,确定 ISMS 的范围,包括任何范围删减的细节和理由。

(2) 根据组织及其业务特点、位置、资产和技术,确定 ISMS 方针,应该做到以下几点:

- 为其目标建立一个框架并为信息安全活动建立整体的方向和原则;
- 考虑业务及法律或法规的要求,及合同的安全义务;
- 建立组织战略和风险管理的环境,在这种环境下,建立和维护 ISMS;
- 建立风险评价的准则;
- 获得管理者批准。

(3) 定义风险评估方法。

- 识别适用于 ISMS 的风险评估方法学和信息安全要求。选择的风险评估方法学应确保风险评估有一个定义清晰的范围,并能产生可比较的和可再现的结果;
- 建立可接受风险的准则;
- 风险评估具有不同的方法学。在 ISO/IEC TR 13335-3(IT 安全管理指南:IT 安全管理技术)中描述了风险评估方法学的例子。

(4) 识别风险。

- 识别 ISMS 范围内的资产及其责任人;
- 识别资产所面临的威胁;
- 识别可能被威胁利用的脆弱性;
- 识别机密性、完整性和可用性遭到破坏所造成的影响。

(5) 分析评价风险。

- 评估安全失误可能造成的对组织的影响,考虑资产的机密性、完整性和可用性遭到破坏所造成的后果;
- 评估由主要威胁、脆弱性导致安全失误的现实可能性,及其对资产的影响和当前所实施的控制措施;
- 评估风险的级别;
- 确定风险是否可接受,或者是否需要使用所建立的风险接受准则进行处理。

(6) 识别和评价风险处理的可选措施可能的行动包括:

- 采用适当的控制措施;
- 在满足组织的方针和风险接受准则的条件下,明确、客观地接受风险;
- 避免风险;
- 转移相关业务风险到其他方,如:保险、供应商等。

(7) 选择控制目标和处理风险的控制措施。

应选择控制目标和控制措施满足风险评估和风险处理过程所识别的需求。选择应考虑可接受风险的准则、法律法规和合同要求。

在 ISMS 的实施和运行阶段,应该做到:

(1) 识别合适的管理行动和确定管理信息安全风险的职责与优先顺序,即制定风险处理计划。

(2) 实施风险处理计划以达到已识别的控制目标,包括资金安排、角色和职责的分配。

(3) 实施所选择的控制措施,以满足控制目标的要求。

(4) 确定如何测量所选择的控制措施或控制措施集的有效性,并指明如何使用以评

估控制有效性,并产生可比较的和可再现的结果。

(5) 实施培训和提高意识的计划。

(6) 管理运行过程。

(7) 管理资源。

(8) 实施能够迅速检测和响应安全事件的程序和其他控制措施。

在 ISMS 的检查阶段,应该做到:

(1) 执行监视程序和其他控制措施,目的是:

- 及时检测处理结果中的错误;
- 及时识别失败的和成功的安全违规和事件;
- 使管理层确定,分配给人员的安全活动或通过信息技术实施的安全活动是否被如期执行;
- 使用有效性测量帮助检测安全违规;
- 确定反映业务的优先顺序的安全违规的解决措施。

(2) 在考虑安全审核结果、安全事故、所有相关方的建议和反馈的基础上,进行 ISMS 有效性的定期评审,包括安全方针和安全目标的符合性的评审和安全控制措施的评审。

(3) 测量控制的有效性以验证是否满足安全要求。

(4) 评审残余风险和可接受风险的级别,需要考虑以下方面的变化情况:

- 组织;
- 技术;
- 业务目标和过程;
- 已经识别的威胁;
- 已经实施的控制措施的有效性;
- 外部事件,如法律或法规环境的变更、合同责任的变更和社会环境的变更。

(5) 按计划规定的时间间隔,对 ISMS 进行内部审核(注:内部审核,又称第一方审核,由组织自身或代表组织的一方为内部目的而自行实施)。

(6) 定期(至少每年 1 次)对 ISMS 进行管理评审,以确保 ISMS 范围保持适宜,ISMS 过程的改进已经识别。

(7) 记录可能对 ISMS 的效率和效果有影响的行动和事件。

此外,为了保持和改进 ISMS,还应该做到以下几点:

(1) 实施已识别的 ISMS 改进措施。

(2) 采取合适的纠正和预防措施,并从其他组织的安全经验和本组织的经验中吸取教训。

(3) 与所有相关方以适当详细的级别沟通结果和行动,合乎环境要求,需要时,商定

如何进行。

（4）确保改进达到了预期目标。

6.4.2　ISO 27000 系列

信息安全管理体系（Information Security Management System，ISMS）是 ISO 发展的一个信息安全管理标准族。

2005 年 10 月，BS 7799-2 正式成为 ISO 27001。这是建立信息安全管理体系（ISMS）的一套规范（Specification for Information Security Management Systems），其中详细说明了建立、实施和维护信息安全管理体系的要求，可用来指导相关人员去应用 ISO/IEC 17799，其最终目的，在于建立适合企业需要的信息安全管理体系。

ISO 27001 为两个部分：ISO 27001-1，信息安全管理实施细则；ISO 27001-2，信息安全管理体系规范。第一部分主要是给负责开发的人员作为参考文档使用，从而在他们的机构内部实施和维护信息安全；第二部分详细说明了建立、实施和维护信息安全管理系统的要求，指出实施组织需遵循某一风险评估来鉴定最适宜的控制对象，并对自己的需求采取适当的控制。

ISO 已为信息安全管理体系标准预留了 ISO/IEC 27000 系列编号，类似于质量管理体系的 ISO 9000 系列和环境管理体系的 ISO 14000 系列标准。

规划的 ISO 27000 系列包含下列标准：

（1）ISO 27000——“Information security management system fundamentals and vocabulary”（《信息安全管理体系原理和术语》）

该标准主要用于阐述 ISMS 的基本原理和术语。

（2）ISO 27001——“Information security management system requirements”（《信息安全管理体系要求》）

该标准源于 BS 7799-2，主要提出 ISMS 的基本要求，已于 2005 年 10 月正式发布。

（3）ISO 27002——“Code of practice for information security management”（《信息安全管理实践规则》）

该标准将取代 ISO/IEC 17799：2005，2007 年 4 月实施。

（4）ISO 27003——“Information security management systems implementation guidance”（《信息安全管理体系实施指南》）

该标准将为 ISMS 的建立、实施、维持、改进提供指导，目前还在开发中。

（5）ISO 27004——“Information security management measurements and metrics”（《信息安全管理测量与指标》）

该标准阐述信息安全管理的测量和指标，用于测量信息安全管理的实施效果，目前还

在开发中。

(6) ISO 27005——"Information security risk management"(《信息安全风险管理》)

该标准以 BS 7799-3 和 ISO 13335 为基础,2008 年 6 月已发布。

(7) ISO 27006——"Information technology-Security techniques-Requirements for bodies providing audit and certification of information security management systems"(《信息安全管理体系审核认证机构要求》)

该标准对提供 ISMS 认证的机构提出要求,所有提供 ISMS 认证服务的机构需要按照该标准的要求证明其能力和可靠性,2007 年 2 月已发布。

(8) ISO 27007——"Guidelines for information security management"(《信息安全管理体系审核指南》)

给出了信息安全管理体系审核指南,已经发布了标准草案。

6.4.3 ISO 27001 在我国的试点

为了了解国际上通用的信息安全管理标准 ISO/IEC 27001:2005《信息安全管理体系要求》和 ISO/IEC 17799:2005《信息安全管理实用规则》是否适合我国的具体情况、在不同的行业是否具有适用性和合理性,我国从 2006 年 3 月开始启动了"信息安全管理标准应用(ISMS)试点"工作。该项工作用半年时间对税务、证券等重要信息系统部门(行业)以及北京市、上海市、武汉钢铁集团等 5 个单位共 7 个系统进行了深入调查,各试点单位的实施效果如下。

1. 深圳证券交易所

深圳证券交易所结合已经实施或正在实施的 ITMS、BCP、CMMI 等工作,历时 6 个月,ISMS 自 2006 年 11 月开始试运行。

(1) 建立了符合 ISO/IEC 27001:2005 要求的、文件化的 ISMS,编制完成了四级体系文件(包括记录表单等)共计 149 份。

(2) 试点工作促进深交所建立了 3 年信息安全规划,推动了深交所"两网隔离工程"的实施,初步建立了实施 ISMS 软件的原型。

(3) 探索出一个在证券行业有效实施 ISMS 的方法——BHTP,即 B 为业务与策略、H 为人员与管理、T 为技术与产品、P 为流程与体系;并从 ISMS 实施方式、实施范围、实施预算等各个方面对证券行业实施 ISMS 提出了具体建议。

(4) 验证了 ISMS 标准在证券行业的适用性,并分析了 ISMS 的标准的优势和缺陷。

2 北京公积金管理中心

北京公积金管理中心与技术支撑单位一起,结合北京公积金的实际情况,将试点工作目标细化为 5 项,历时 8 个月,ISMS 自 2006 年 11 月开始运行,完成了试点工作。

（1）通过试点工作，更准确、全面地把握了安全现状，在北京公积金建立了切合自身的、文件化的 ISMS，形成了包括信息安全管理手册、程序文件以及记录文件在内的三级体系文件共计 112 份。

（2）探索和研究了适合 ISMS 建设的风险评估方法，结合电子政务的等级保护工作，探索了等级化信息安全管理体系建立的流程和步骤。

（3）通过试点，建立了信息安全管理的组织机构并明确了责任，任命了信息安全管理委员会主任、管理者代表和内审员。

3. 北京市海淀信息办

北京海淀结合已经实施的 ISO 9000、等级保护、风险评估等工作，将试点工作目标细化为 5 项，历时 8 个月，ISMS 自 2006 年 11 月开始试运行，完成了试点工作。

（1）建立了符合 ISO/IEC 27001：2005 要求的、文件化的 ISMS，编制完成了三级体系文件（包括记录表单等）共计 79 份。

（2）探索和研究了 ISMS 与风险评估和等级保护的关系。参考《电子政务信息安全等级保护实施指南》，先按照等级保护制度对其进行定级，然后将对应的等级要求体现到方针中；参考《信息安全风险评估指南》确定了 ISMS 要求的风险评估方法。

（3）探索和研究了 ISMS 与 QMS（质量管理体系）整合的方法，充分考虑了已经实施并通过了认证的 QMS，在组织机构、内部审核、管理评审、文件控制、预防和纠正措施控制等方面，使两个管理体系实现了有机的整合。

4. 上海市医疗保险信息中心

上海市医疗保险信息中心与其技术支撑单位上海市信息安全测评认证中心一起，于 2006 年 12 月完成了试点工作方案确定的目标。

（1）通过试点工作，依据 ISO/IEC 27001：2005 建立了相对完整的信息安全管理体系。

（2）对 ISMS 标准实施与单位具体情况相结合方面做出了积极的实践并积累了经验，包括 ISMS 与医保信息系统状况融合和 ISMS 与已经实施的 QMS（质量管理体系）的融合。

（3）检验了 ISMS 标准的适用性。试点工作证明 ISO/IEC 27001：2005 是适用的，并对 ISO/IEC 17799：2005 一些具体控制措施也做出了适用性分析。

5. 上海市宝山区信息委

上海市宝山区信息委与其技术支撑单位上海市信息安全测评中心经过 7 个多月的共同努力，完成了试点工作方案确定的目标。

（1）建立了体系化的管理规范。从宝山区电子政务平台、接入单位和信息委三个不

同层面,分别建立了《上海宝山电子政务平台信息安全管理规范》文件 7 份、《宝山电子政务平台接入单位信息安全管理规范》文件 10 份和《上海宝山信息委信息安全管理规范》文件 18 份。

(2) 改善了宝山区系统安全状况。区信息委对在试点过程中发现的安全风险,已立项并投入大量资金,实施"改进"措施,从而大大提升了宝山电子政务系统的安全性。

(3) 对 ISMS 与风险评估和等级保护工作的关系进行了研究和探索,对政府部门建立 ISMS 提出了建议。

6. 福建地方税务局

福建地方税务局与技术支撑单位中国信息安全测评认证中心一起,周密计划、认真组织,完成了试点工作。

(1) 通过试点,对福建地税与惠普公司合作根据 BS 7799(ISO/IEC 17799:2000)完成的 19 份安全策略及其实施文档,对照 ISO/IEC 27001:2005,进行了全面整理,并新编制体系文件 11 份,建立了 ISMS。

(2) 加强了 ISMS 的推广与实施,计划以正式文件的形式下发 ISMS 体系文档,并根据税务系统的实际岗位需要制定了《办税服务厅工作人员安全手册》等四类工作人员的安全手册。

(3) 根据 ISMS 体系文件中机房安全管理守则、外部访问安全策略、内部访问安全策略等文件的规定,规范了 ISMS 的运行记录。

(4) 对 ISMS 标准的适用性进行了分析,福建地税认为 ISO/IEC 2700:2005 是一个基于企业信息安全管理的通用标准,并不完全适合我们国内的实际情况,特别是税务系统这样的政府机关部门,引进时要进行本地化工作。另外,也对 ISMS 与风险评估、等级保护的关系进行了研究和探索。

7. 武汉钢铁(集团)公司

武汉钢铁(集团)公司与技术支撑单位上海三零卫士信息安全有限公司一起,对试点工作进行周密计划、精心组织,将武钢的试点工作目标细化分解为九项,历时 8 个月完成了试点工作。

(1) 编制了 31 份信息安全管理体系文件,按照 ISO/IEC 27001:2005 建立了武钢信息安全管理体系,为下一步通过 ISMS 认证奠定了基础。

(2) 实施了风险评估和风险处理。通过试点工作,对武钢包括应用系统、主干网、接入单位在内的关键信息资产进行了量化风险评估,分析了存在的安全风险,并编制和实施了风险处理计划付诸实施。

(3) 对信息安全管理标准应用进行了探索。通过试点,武钢认为 ISO/IEC 27001:

2005 和 ISO/IEC 17799:2005 这两个 ISMS 标准总体上是适用的，但一些条款应考虑与我国实际情况相结合。

(4) 对同类系统建立和实施 ISMS 提供了建议，包括明确 ISMS 的实施范围，以信息系统可用性保障作为实施重点，注重质量管理体系与 ISMS 体系的融合等。

6.5 信息安全法律法规

6.5.1 国际信息安全法律法规现状

在信息安全问题和犯罪现象日益增多的背景下，信息安全立法与执法在世界范围内受到了更多的重视。

目前，有关信息安全的国际性法律、决议和公约主要有：1992 年联合国各成员国签署的《国际电信联盟组织法》；1998 年联合国大会通过的“关于信息和传输领域成果只用于国际安全环境”的决议；欧洲委员会于 2000 年制定的《打击计算机犯罪公约》。其中，《打击计算机犯罪公约》是世界上第一个以打击黑客为目标的国际性公约，包括美国等 40 多个国家已经加入了这个公约。

1. 美洲

在美洲，美国和加拿大在信息安全法律法规的制定与实施方面起步早，成果也较为显著。

美国是迄今为止信息安全法律法规(包括美国国会法案)最多的国家。这些法律法规构成了相对完善的法律体系，为维护美国的信息安全秩序发挥了关键作用。该法律体系一方面受美国国家政体所具有的三权分立的特点的影响，另一方面也受日新月异的信息安全技术的影响。在三权分立的政体之下，美国的立法和司法程序相对独立又相互制约，信息安全的立法与司法活动本身也相应地处于不断调整、完善的过程，一个有待通过的法案往往既在国会经历多次争论，又在民间引起强烈反响。即使对于政府已经颁布实施的法律，如果民间机构或民众提出强烈反对并提交国家最高法院就其合理性和公正性等内容进行裁决，也有可能被推翻。例如，美国曾经于 1996 年 2 月颁布了《正当通信法令》，但是一些传媒机构和民权团体提出该法令违反了宪法所授予的资讯自由，提请最高法院裁决，结果最高法院于 1996 年 6 月便推翻了这部法令，使美国联邦政府管制色情资讯的努力遭到重大挫折。这件事情表明在美国式的民主下，Internet 的法制管理困难尚多。

与美国国家信息安全立法和司法活动密切相关的国家信息安全工作部门主要有：国家安全局(NSA)、中央情报局(CIA)、联邦调查局(FBI)、总统关键基础设施保护委员会

(PCCIB)、国家基础设施保护中心(NIPC)、国家计算机安全中心、基础设施威胁评估中心、最高法院等。

美国对国家信息安全尤其重视，其行政法、刑法、诉讼法等十分全面。从法规体系上说，在行政法方面，1987年推出的《计算机安全法》定义了对联邦计算机系统中的敏感资料的保护。修改后的这部《计算机犯罪法》在20世纪80年代末至90年代初被美国各州作为制定其地方法规的重要依据。这些地方法规结合当地的具体情况，确立了包括计算机服务盗窃罪、侵犯知识产权罪、破坏计算机设备或配置罪、计算机欺骗罪、通过欺骗获得电话或电报服务罪、计算机滥用罪、计算机错误访问罪、非授权计算机使用罪在内的多种罪名。在刑法方面，1984年出台了《计算机诈骗和滥用法》，1987年联邦计算机犯罪法正式颁布。在诉讼法方面，《联邦证据法》对计算机证据做出了相应的规定。此外，美国早已制定出信息战框架，例如《信息战条令》、《2010年联合构想》等，并在实战中得到了检验。

2 欧洲

与美洲和亚洲不同，欧洲多数国家长期以来一直在积极地推进欧洲一体化进程，其信息安全法律法规的主体也在很多情况下超越了单独某个国家的范畴，与多个欧洲国家间的利益协调相关，通常由在欧洲范围内具有较强影响力的政府间组织出面负责。

欧共体就是这样一个政府间组织。为了确保在欧共体范围内正常地进行信息市场运作，该组织确立了一系列法律法规，具体包括：竞争(反托拉斯)法，产品责任、商标和广告规定，知识产权保护法，保护软件、数据和多媒体产品及在线版权法，数据保护法，跨境电子贸易法，以及其他涉及税收和司法问题的法律法规。在欧共体范围内，如果这些法律法规与欧共体成员国原有国家法律相矛盾，则必须以欧共体的法律法规为准。

欧共体成员国从20世纪70年代末到90年代初，先后制定并颁布了各自有关数据安全的法律。例如，瑞士早在1973年就通过了世界上第一部保护计算机的法律。德国1996年出台《信息和通信服务规范法》即《多媒体法》，该法被认为是世界上第一部规范Internet的法律。

此外，俄罗斯也在信息安全立法执法方面做了很多工作，紧密围绕国家信息安全制定了一系列法律和规范，例如《参与国际信息交流法》、《俄联邦信息、信息化和信息保护法》等。2000年，俄罗斯总统普京签发的《俄联邦信息安全学说》包括4方面内容：信息安全领域的国家利益；保障信息安全的方法；信息安全保障国家政策的基本原则和实施这一政策的首要措施；信息安全保障体系的主要职能和组成部分。

3. 亚洲

在亚洲，本节主要介绍新加坡和日本的信息安全法律法规情况。

新加坡现有的信息安全法律法规主要有互联网分类许可证制度。

日本现有的信息安全法律法规主要是由通产省编制的一套准则，内容是防止越权访问计算机网络。这套准则建议计算机使用者避免将出生日期和电话号码作为计算机口令，并建议计算机用户定期更改口令。同时，它也提出应该像努力防止计算机病毒扩散一样，防止黑客窃取、替换和破坏网络上的数据。2000 年年底，日本防卫厅公开发表的《信息军事革命手册》对信息安全给予高度重视，强调要采取一切措施防止系统瘫痪，确保信息安全。

6.5.2 中国信息安全法律法规现状

我国在信息安全方面也已经制定了一些法律和规定。这些法规有国家制定的和分管部门制定的，也有一些行业制定了自己的有关信息安全的规定。

这些位于不同层面的法律法规有着各自不同的侧重点。其中，国家宪法从国家根本大法的高度规定了公民的基本权利和义务；国家安全法、保密法从国家安全、保守国家秘密的角度提出法律要求；专利法、著作权法从保护知识产权的角度制定了法律约束；电信条例对于网络基础设施的建设、运行、安全、服务、利益给出了规定；计算机信息系统安全保护条例、商用密码管理条例则直接对信息安全提出了法规要求；标准化法、产品质量法的有关规定对于在信息安全领域制定和实施标准，保证产品质量有约束力；进一步加强互联网上网服务营业场所管理的通知、互联网信息服务管理办法等对于网络化公共服务提出了要求；全国人民代表大会常务委员会关于维护互联网安全的决定、1997 年修订的刑法则对于行为规范的法律界限给出了明确的界定。

1. 国家法律

在我国现有的国家法律中，信息安全相关法律法规有：

(1) 中华人民共和国保守国家秘密法(1988.09.05)。

(2) 中华人民共和国标准化法(1988.12.29)。

(3) 中华人民共和国产品质量法(2000.07.08)。

(4) 中华人民共和国反不正当竞争法。

(5) 中华人民共和国国家安全法(1993.02.22)。

(6) 中华人民共和国人民警察法(1995.02.28)。

(7) 中华人民共和国宪法。

(8) 中华人民共和国刑法。

(9) 中华人民共和国刑事诉讼法。

(10) 中华人民共和国行政处罚法。

(11) 中华人民共和国著作权法。

(12) 中华人民共和国专利法。

(13) 中华人民共和国海关法。

(14) 中华人民共和国商标法。

(15) 中华人民共和国电子签名法(2005.04.01)。

(16) 全国人民代表大会常务委员会关于维护互联网安全的决定。

其中,(1)、(5)、(15)、(16)是信息安全法律法规。

2 国家行政法规

在我国现有的国家行政法规中,信息安全相关行政法规有:

(1)《中华人民共和国产品质量认证管理条例》(1991.05.07)。

(2) 国务院第 84 号令——《计算机软件保护条例》(1991.06.04)。

(3) 国务院第 147 号令——《中华人民共和国计算机信息系统安全保护条例》(1994.02.18)。

(4) 国务院第 195 号令——《中华人民共和国计算机信息网络国际联网管理暂行规定》。

(5) 国务院第 273 号令——《商用密码管理条例》(1999.10.07)。

(6) 国务院第 291 号令——《中华人民共和国电信条例》。

(7) 国务院第 292 号令——《互联网信息服务管理办法》。

(8)《中华人民共和国计算机信息网络国际联网管理暂行办法》(1996 年 2 月 1 日中华人民共和国国务院令第 195 号发布,根据 1997 年 5 月 20 日《国务院关于修改[中华人民共和国计算机信息网络国际联网管理暂行规定]的决定》修正)。

(9)《全国人民代表大会常务委员会关于维护互联网安全的决定》(2000 年 12 月 28 日,第九届全国人民代表大会常务委员会第十九次会议通过)。

(10)《中华人民共和国电信条例》(2000 年 9 月 20 日国务院第 31 次常务会议通过)。

(11)《国务院办公厅关于进一步加强互联网上网服务营业场所管理的通知》(2002.04.03)。

(12)《国家信息化领导小组关于加强信息安全保障工作的意见》(中办发[2003]27 号),2003 年,中央办公厅、国务院办公厅转发。

(13)《关于信息安全等级保护工作的实施意见》,2004 年 9 月 15 日,已经国家网络与信息安全协调小组讨论通过。

(14) 国务院第 468 号令——《信息网络传播权保护条例》,2006 年 5 月 10 日国务院第 135 次常务会议通过,2006 年 7 月 1 日起施行。

(15)《信息安全等级保护管理办法(试行)》,2006 年 3 月 1 日起施行。

(16)《信息安全等级保护管理办法》已于 2007 年 6 月 22 日,由公安部、国家保密局、国家密码管理局、国务院信息化工作办公室等国家四部委制定完成并审批通过,并发布施行。

其中,(3)、(5)、(9)、(12)～(14)、(16)是信息安全行政法规。

3. 部门规章

在我国现有的部门规章中,信息安全相关规章有:

1) 公安部

(1)《公安部关于对与国际联网的计算机信息系统进行备案工作的通知》(1996.01.29)。

(2) 第 32 号令——《计算机信息系统安全产品检测和销售许可证管理办法》(1997.06.28)。

(3) 第 33 号令——《计算机信息网络国际联网安全保护管理办法》(1997.12.30)。

(4) 第 51 号令——《计算机病毒防治管理办法》(2000.04.26)。

(5) 中华人民共和国公共安全行业标准——计算机信息系统安全专用产品分类原则。

(6) 关于对《中华人民共和国计算机信息系统安全保护条例》中涉及的“有害数据”问题的批复。

(7)《联网单位安全员管理办法(试行)》(公安部第十一局 2000 年 9 月 29 日发布)。

(8)《互联网安全保护技术措施规定》(2005 年 11 月 24 日,公安部部长办公会审议通过,12 月 13 日正式颁布,2006 年 3 月 1 日起实施)。

(9)《互联网安全保护技术措施概况规定》(2006.03.01)。

2) 国家保密局

有《计算机信息系统国际联网保密管理规定》(2000)等。

3) 国家密码管理局(原国家密码管理委员会)

(1)《国家密码管理委员会办公室公告(第一号)》。

(2)《电子认证服务密码管理办法》(2005.04.01)。

4) 国务院新闻办公室

有《互联网站从事登载新闻业务管理暂行规定》等。

5) 新闻出版总署

(1) 新闻出版总署第 11 号令——《电子出版物管理规定》(1998.01.01)。

(2) 关于实施《电子出版物管理暂行规定》若干问题的通知。

(3)《互联网出版管理暂行规定》(2002.06.27)新闻出版总署、信息产业部令(第

17 号)。

6) 信息产业部(包括原邮电部、电子部)

(1)《计算机信息系统集成资质管理办法(试行)》(1999)。

(2)《电信网间互联管理暂行规定》(1997.09.07)。

(3)《互联网电子公告服务管理规定》(2000.10.27)。

(4)《软件产品管理办法》(2000.10.27)。

(5)《关于互联网中文域名管理的通告》。

(6)《互联网出版管理暂行规定》(2002.06.07)新闻出版总署、信息产业部令(第17 号)。

(7)《中国互联网络域名管理办法》(2002.08.01)。

(8)《互联网上网服务营业场所管理条例》(2002.11.15)。

(9)《软件企业认定标准及管理办法(试行)》。

(10)《关于处理恶意占用域名资源行为的批复》。

(11)《互联网上网服务营业场所管理办法》(2002.11.15)。

(12) 电子认证服务管理办法(2005.04.01)。

(13)《非经营性互联网信息服务备案管理办法》(2005.03.20)。

(14)《互联网新闻信息服务管理》(2005.09.25) 国务院新闻办公室、信息产业部。

(15)《互联网电子邮件服务管理办法》(2006.03.30)。

(16)《互联网交换中心网间结算办法》,2006 年 10 月 23 日发布,2006 年 11 月 1 日起施行。

(17)《计算机信息网络国际联网出入口信道管理办法》。

(18)《通信建设市场管理办法》(1995.04.11)。

(19)《通信行政处罚程序暂行规定》(1995.10.27)。

(20)《中国公用计算机互联网国际联网管理办法》。

(21)《中国公众多媒体通信管理办法》(1997.12.01)。

(22)《中国金桥信息网公众多媒体信息服务管理办法》。

7) 中华人民共和国国家科学技术委员会

《科学技术保密规定》(1995 年 1 月 6 日中华人民共和国国家科学技术委员会国家保密局令第 20 号发布)。

8) 最高人民法院

(1)《关于审理扰乱电信市场管理秩序案件集体应用法律若干问题的解释》。

(2)《关于审理设计计算机网络域名民事纠纷案件适用法律若干问题的解释》。

(3)《关于审理扰乱电信市场管理秩序案件集体应用法律若干问题的解释》

(2000 年)。

9) 广电总局

关于加强通过信息网络向公众传播广播电影电视类节目管理的通告(1999.10)。

10) 国务院信息办

(1)《中国互联网络域名注册实施细则》等。

(2)《中国互联网络域名注册暂行管理办法》等。

11) 教育部

《教育网站和网校暂行管理办法》等。

12) 证监会

(1)《网上证券委托暂行管理办法》等。

(2)《证券期货业信息安全保障管理暂行办法》(2005.04.08)。

13) 中国人民银行

《金融机构计算机信息系统安全保护工作暂行规定》(公安部、中国人民银行 1998 年 8 月 31 日发布)。

14) 文化部

(1)《文化部关于加强网络文化市场管理的通知》(2002 年)。

(2)《互联网出版管理暂行规定》(2002.08.01)中国新闻出版总署、中国信息产业部令。

(3)《互联网文化管理暂行规定》(2003.05.10)。

15) 卫生部

《互联网医疗卫生信息服务管理办法》。

16) 国家烟草专卖局

关于印发《烟草行业计算机信息网络安全保护规定》的通知(国烟办[1998]305 号)。

17) 国家质量监督检验检疫总局

关于质检计算机网络系统安全运行管理的暂行规定。

4. 地方性法律法规

在我国现有的地方性法律法规中,信息安全相关地方性法律法规有:

(1)《天津市公共计算机信息网络安全保护规定》。

(2)《河北省电子政务建设总体规划(2003—2007)的通知》。

(3)《山西省计算机安全管理规定》。

(4)《大连市人民政府公共信息网络管理暂行规定》。

(5)《黑龙江省计算机信息系统安全管理规定》。

(6)《上海市关于加强本市政府网站安全建设的试行意见》。
(7)《上海市数字认证管理办法》。
(8)《江苏省计算机信息系统安全保护管理办法》。
(9)《安徽省计算机信息系统安全保护办法》。
(10)《安徽省预防和控制计算机病毒管理暂行办法》。
(11)《福建省关于加强基层文化信息网络安全管理工作的通知》。
(12)《厦门市计算机信息系统安全保护暂行办法》。
(13)《山东省计算机信息系统安全管理办法》。
(14)《青岛市信息化建设管理暂行规定》。
(15)《河南省计算机信息系统安全保护暂行办法》。
(16)《河南省学校计算机信息系统安全管理暂行规定》。
(17)《武汉市电子政务建设管理暂行办法》。
(18)《广东省计算机信息系统安全保护管理规定》。
(19)《广东省计算机信息系统安全保护管理规定实施细则》。
(20)《广东省电子交易条例》。
(21)《广州市电子公文和信息交换管理试行规定》。
(22)《深圳经济特区计算机信息系统公共安全管理规定》。
(23)《海南省数字证书认证管理试行办法》。
(24)《四川省计算机信息系统安全保护管理办法》。
(25)《宁夏回族自治区计算机信息系统保密工作管理规定》。

5. 重要法律法规主要内容介绍

1)《中华人民共和国宪法》相关内容

1982 年 12 月 4 日第五届全国人民代表大会第五次会议通过 1982 年 12 月 4 日全国人民代表大会公告公布施行，根据 1988 年 4 月 12 日第七届全国人民代表大会第一次会议通过的《中华人民共和国宪法修正案》、1993 年 3 月 29 日第八届全国人民代表大会第一次会议通过的《中华人民共和国宪法修正案》、1999 年 3 月 15 日第九届全国人民代表大会第二次会议通过的《中华人民共和国宪法修正案》和 2004 年 3 月 14 日第十届全国人民代表大会第二次会议通过的《中华人民共和国宪法修正案》修正。

宪法总纲中明确了我国的国家性质和社会制度，人民的权力和行使权力的途径、形式和原则。新修订的宪法在明确社会主义的公共财产神圣不可侵犯的同时也提出了公民的合法的私有财产不受侵犯。

宪法明确提出，国家提倡爱祖国、爱人民、爱劳动、爱科学、爱社会主义的公德，在人民

中进行爱国主义、集体主义和国际主义、共产主义的教育，进行辩证唯物主义和历史唯物主义的教育，反对资本主义的、封建主义的和其他的腐朽思想。

国家维护社会秩序，镇压叛国和其他危害国家安全的犯罪活动，制裁危害社会治安、破坏社会主义经济和其他犯罪的活动，惩办和改造犯罪分子。

宪法规定了公民的基本权利和义务。直接与信息化相关的权利有，"中华人民共和国公民的通信自由和通信秘密受法律的保护。除因国家安全或者追查刑事犯罪的需要，由公安机关或者检察机关依照法律规定的程序对通信进行检查外，任何组织或者个人不得以任何理由侵犯公民的通信自由和通信秘密"。

宪法规定，中华人民共和国公民必须遵守宪法和法律，保守国家秘密，爱护公共财产，遵守劳动纪律，遵守公共秩序，尊重社会公德。中华人民共和国公民有维护祖国的安全、荣誉和利益的义务，不得有危害祖国的安全、荣誉和利益的行为。这些都是国家根本大法对公民的基本要求。

2）《中华人民共和国保守国家秘密法》相关内容

1988 年 9 月 5 日中华人民共和国主席令第 6 号公布。

法律指出，国家秘密关系国家的安全和利益，一切国家机关、武装力量、政党、社会团体、企业事业单位和公民都有保守国家秘密的义务。

法律指定，国家保密工作部门主管全国保守国家秘密的工作。

法律提出了保守国家秘密的工作，实行积极防范、突出重点、既确保国家秘密又便利各项工作的方针。

法律阐明国家秘密包括下列秘密事项：

- 国家事务的重大决策中的秘密事项；
- 国防建设和武装力量活动中的秘密事项；
- 外交和外事活动中的秘密事项以及对外承担保密义务的事项；
- 国民经济和社会发展中的秘密事项；
- 科学技术中的秘密事项；
- 维护国家安全活动和追查刑事犯罪中的秘密事项；
- 其他经国家保密工作部门确定应当保守的国家秘密事项。

法律规定，国家秘密的密级分为"绝密"、"机密"、"秘密"三级，"绝密"是最重要的国家秘密，泄露会使国家的安全和利益遭受特别严重的损害；"机密"是重要的国家秘密，泄露会使国家的安全和利益遭受严重的损害；"秘密"是一般的国家秘密，泄露会使国家的安全和利益遭受损害。

法律要求：

各级国家机关、单位对所产生的国家秘密事项，应当按照国家秘密及其密级具体范围

的规定确定密级。对是否属于国家秘密和属于何种密级不明确的事项，由国家保密工作部门，省、自治区、直辖市的保密工作部门，省、自治区政府所在地的市和经国务院批准的较大的市的保密工作部门或者国家保密工作部门审定的机关确定。在确定密级前，产生该事项的机关、单位应当按照拟定的密级，先行采取保密措施。

属于国家秘密的文件、资料和其他物品的制作、收发、传递、使用、复制、摘抄、保存和销毁，由国家保密工作部门制定保密办法。采用电子信息等技术存取、处理、传递国家秘密的办法，由国家保密工作部门会同中央有关机关规定。

对绝密级的国家秘密文件、资料和其他物品，必须采取以下保密措施：

- 非经原确定密级的机关、单位或者其上级批准，不得复制和摘抄；
- 收发、传递和外出携带，由指定人员担任，并采取必要的安全措施；
- 在设备完善的保险装置中保存。

具有属于国家秘密内容的会议和其他活动，主办单位应当采取保密措施，并对参加人员进行保密教育，规定具体要求。

在有线、无线通信中传递国家秘密的，必须采取保密措施。不准使用明码或者未经中央有关机关审查批准的密码传递国家秘密。不准通过普通邮政传递属于国家秘密的文件、资料和其他物品。

法律规定，违反本法规定，故意或者过失泄露国家秘密，情节严重的，依照刑法第一百八十六条的规定追究刑事责任。违反本法规定，泄露国家秘密，不够刑事处罚的，可以酌情给予行政处分。为境外的机构、组织、人员窃取、刺探、收买、非法提供国家秘密的，依法追究刑事责任。

3)《中华人民共和国刑法》相关内容

1979 年 7 月 1 日第五届全国人民代表大会第二次会议通过，1997 年 3 月 14 日第八届全国人民代表大会第五次会议修订。

在 1997 年修订的刑法中，增加了几个直接与计算机犯罪有关的罪行、罪名及其量刑规定，它们是：

第二百八十五条　违反国家规定，侵入国家事务、国防建设、尖端科学技术领域的计算机信息系统的，处三年以下有期徒刑或者拘役。

第二百八十六条　违反国家规定，对计算机信息系统功能进行删除、修改、增加、干扰，造成计算机信息系统不能正常运行，后果严重的，处五年以下有期徒刑或者拘役；后果特别严重的，处五年以上有期徒刑。

违反国家规定，对计算机信息系统中存储、处理或者传输的数据和应用程序进行删除、修改、增加的操作，后果严重的，依照前款的规定处罚。

故意制作、传播计算机病毒等破坏性程序，影响计算机系统正常运行，后果严重的，依

照第一款的规定处罚。

第二百八十七条 利用计算机实施金融诈骗、盗窃、贪污、挪用公款、窃取国家秘密或者其他犯罪的，依照本法有关规定定罪处罚。

这是我国第一次在刑法中明确提出了与信息安全相关的罪名及罚则。与信息安全有关的犯罪行为远不止这样几条，因此，当前在许多犯罪案件的处理中，尚需要在目前刑法条款中进行类比解释。

4）《全国人民代表大会常务委员会关于维护互联网安全的决定》相关内容

2000 年 12 月 28 日，第九届全国人民代表大会常务委员会第十九次会议通过。

决定指出，我国的互联网，在国家大力倡导和积极推动下，在经济建设和各项事业中得到日益广泛的应用，使人们的生产、工作、学习和生活方式已经开始并将继续发生深刻的变化，对于加快我国国民经济、科学技术的发展和社会服务信息化进程具有重要作用。同时，如何保障互联网的运行安全和信息安全问题已经引起全社会的普遍关注。

为了兴利除弊，促进我国互联网的健康发展，维护国家安全和社会公共利益，保护个人、法人和其他组织的合法权益，决定在保障互联网的运行安全，维护国家安全和社会稳定，维护社会主义市场经济秩序和社会管理秩序，保护个人、法人和其他组织的人身、财产等合法权利等方面列举了构成犯罪的行为，并提出要依照刑法有关规定追究刑事责任。

在为了保障互联网的运行安全方面，决定列举的构成犯罪的行为有：

（1）侵入国家事务、国防建设、尖端科学技术领域的计算机信息系统。

（2）故意制作、传播计算机病毒等破坏性程序，攻击计算机系统及通信网络，致使计算机系统及通信网络遭受损害。

（3）违反国家规定，擅自中断计算机网络或者通信服务，造成计算机网络或者通信系统不能正常运行。

在为了维护国家安全和社会稳定方面，决定列举的构成犯罪的行为有：

（1）利用互联网造谣、诽谤或者发表、传播其他有害信息，煽动颠覆国家政权、推翻社会主义制度，或者煽动分裂国家、破坏国家统一。

（2）通过互联网窃取、泄露国家秘密、情报或者军事秘密。

（3）利用互联网煽动民族仇恨、民族歧视，破坏民族团结。

（4）利用互联网组织邪教组织、联络邪教组织成员，破坏国家法律、行政法规实施。

为了维护社会主义市场经济秩序和社会管理秩序方面，决定列举的构成犯罪的行为有：

（1）利用互联网销售伪劣产品或者对商品、服务作虚假宣传。

（2）利用互联网损害他人商业信誉和商品声誉。

（3）利用互联网侵犯他人知识产权。

(4) 利用互联网编造并传播影响证券、期货交易或者其他扰乱金融秩序的虚假信息。

(5) 在互联网上建立淫秽网站、网页,提供淫秽站点链接服务,或者传播淫秽书刊、影片、音像、图片。

为了保护个人、法人和其他组织的人身、财产等合法权利方面,决定列举的构成犯罪的行为有:

(1) 利用互联网侮辱他人或者捏造事实诽谤他人。

(2) 非法截获、篡改、删除他人电子邮件或者其他数据资料,侵犯公民通信自由和通信秘密。

(3) 利用互联网进行盗窃、诈骗、敲诈勒索。

决定提出的四类 14 条犯罪行为,补充了 1997 年修改的刑法中对信息犯罪行为定罪的不足,对当前治理和打击信息犯罪行为起到了重要的作用。

决定指出:利用互联网实施违法行为,违反社会治安管理,尚不构成犯罪的,由公安机关依照《治安管理处罚条例》予以处罚;违反其他法律、行政法规,尚不构成犯罪的,由有关行政管理部门依法给予行政处罚;对直接负责的主管人员和其他直接责任人员,依法给予行政处分或者纪律处分。利用互联网侵犯他人合法权益,构成民事侵权的,依法承担民事责任。

各级人民政府及有关部门要采取积极措施,在促进互联网的应用和网络技术的普及过程中,重视和支持对网络安全技术的研究和开发,增强网络的安全防护能力。有关主管部门要加强对互联网的运行安全和信息安全的宣传教育,依法实施有效地监督管理,防范和制止利用互联网进行的各种违法活动,为互联网的健康发展创造良好的社会环境。从事互联网业务的单位要依法开展活动,发现互联网上出现违法犯罪行为和有害信息时,要采取措施,停止传输有害信息,并及时向有关机关报告。任何单位和个人在利用互联网时,都要遵纪守法,抵制各种违法犯罪行为和有害信息。人民法院、人民检察院、公安机关、国家安全机关要各司其职,密切配合,依法严厉打击利用互联网实施的各种犯罪活动。要动员全社会的力量,依靠全社会的共同努力,保障互联网的运行安全与信息安全,促进社会主义精神文明和物质文明建设。

6.6 小结

本章主要介绍了风险评估、信息安全管理标准 ISO/IEC 17799、信息安全等级保护、信息安全管理体系,以及信息安全法律法规,重点讲述了风险评估的概念与步骤,17799 标准的主要内容,信息安全等级保护制度,信息安全管理体系各个阶段需要进行的主要事

情和 ISO 27001 在我国的试点情况。在法律法规方面,我们总结了国际和中国的相关现状,列出了目前我国正在执行的相关国家法律、国家行政法规、部门规章和地方性法律法规,并介绍了几个重要法律法规的主要内容。

习 题

1. 什么是风险评估? 简述风险、威胁、脆弱性各自的定义和相互间的关系。

2. 风险评估的主要流程是什么? 风险评估在信息安全管理体系中的作用是什么?

3. ISO/IEC 17799:2005、ISO/IEC TR 13335 和 SSE-CMM 都有哪些异同之处?

4. 我国“信息安全等级保护”的定义是什么?

5. 在我国,实施等级保护应该遵从什么工作程序?

6. PDCA 模型和 ISO 27000 标准族是什么关系?

7. ISO 27001 和 ISO 27002 有什么关联? 当企业实施信息安全管理时,两者各扮演了什么角色?

8. 我国有无和 ISO 17799 相对应的国家标准? 如果有,它和 ISO 17799 有什么不同之处?

9. 了解你所在行业的信息安全相关管理标准。

10. 美国的国家信息安全立法和司法活动相关工作部门主要有哪几个? 请了解至少一家部门的相关最新动态(例如,是否新成立了什么具体的职能机构? 新近颁布了什么法令? 是否对某个案件的处理办法存在争议? 某项新规定的实施效果如何? 等等)。

11. 了解你所在地区的信息安全相关法律法规。

12. 搜集并简述 2 或 3 个我国境内的信息安全事件案例,并说明与其相关的我国信息安全法律法规在事件处理过程中的实施情况。

13. 搜集并简述一个其他国家的信息安全事件案例,并说明与之相关的信息安全法律法规在事件处理过程中的实施情况。

第7章 人员能力成熟度模型

7.1 产生背景

7.1.1 关于能力成熟度模型

能力成熟度模型(Capability Maturity Model,CMM),顾名思义,就是用来测量某种能力成熟程度高低的模型。

有关能力成熟度模型的研究,最早起源于美国军方。当时,他们为保证采购的军用软件具备合格的质量,出资并委托美国卡内基梅隆大学开展有关的研究工作。截至目前,卡内基梅隆大学的研究人员已经提出了多种能力成熟度模型,在该领域的研究工作上取得了主导地位。

确切地讲,一个能力成熟度模型是用来描述有效过程特性的要素的结构化集合。通常,一个能力成熟度模型可以被用作一个基点,以此来比较和评价不同组织具备某种能力可能达到的效果。该模型可以提供:

(1) 一个进行这种比较和评价的参考起点。

(2) 共性经验能够带来的利益。

(3) 一种通用的语言和一个共享的洞察力。

(4) 一个优先行动的架构。

(5) 一个为实现组织机构的进步而定义的可行方法。

这表明,采纳能力成熟度模型的思路,更有利于对某种行为的实施情况进行评估和加以改进。

能力成熟度模型可以用于不同的研究领域,例如,系统工程、系统安全工程、安全评估等。目前比较通用的能力成熟度模型都是由卡内基梅隆大学的研究人员提出来的,具体有:

(1) 系统工程能力成熟度模型(SE-CMM)1.1版(1995年11月发布)。

(2) 系统安全工程能力成熟度模型(SSE-CMM)2.0版(1999年4月发布)。

(3) 信息安全评估能力成熟度模型(IA-CMM)(2001年发布,2003年改名为“信息安

全保障能力成熟度模型”)。

(4) 软件能力成熟度模型(SW-CMM2)。

(5) 整合产品开发能力成熟度模型(IPD-CMM4)。

(6) 软件采购能力成熟度模型(SA-CMM5)。

(7) 整合的能力成熟度模型(CMMI6)。

(8) 人员能力成熟度模型(P-CMM)1.0 版(1995 年 9 月发布)。

(9) 人员能力成熟度模型(P-CMM)2.0 版(2001 年 7 月发布)。

有统计资料表明,自 1993 年至 2001 年 7 月,全球共有 1505 个组织,8134 个专案向美国卡内基梅隆大学的软件工程研究院(Software Engineering Institute,SEI)提出了鉴定报告申请,其中有 3.5%(大约 52 个组织)达到了级别 5(优先级)。

其中,SSE-CMM 是系统安全工程能力成熟度模型(Systems Security Engineering Capability Maturity Model)的缩写,描述了一个机构的安全工程过程必须包含的本质特征。2002 年 3 月 18 日,SSE-CMM 被国际标准化组织接纳为国际标准(ISO/IEC 21827 “信息技术—系统安全工程—能力成熟度模型”)。

SSE-CMM 覆盖了以下内容:

(1) 工程的完整生命周期,具体包括开发、运行、维护和终止。

(2) 整个机构的情况,包括其中的管理活动、组织活动和工程活动情况。

(3) 与其他学科和领域(例如,系统、软件、硬件、人的因素和测试工程以及系统的管理、运行和维护)彼此间的相互作用。

(4) 与其他机构的相互作用,包括进行采办、系统管理、认证、认可和评估的机构。

在 SSE-CMM 模型的描述包含:

(1) 基本原理(方法学)和体系结构。

(2) 对模型的高层综述。

(3) 该模型的正确使用方法建议。

(4) 实施 SSE-CMM 的方法建议。

(5) 模型属性。

(6) 开发该模型的要求。

SSE-CMM 主要是对信息安全工程能力进行评估,是信息安全工程实施的标准化评估准则。这就决定了两点:

(1) 它与其他工程方法不同,SSE-CMM 在规定特定的工程过程和步骤时,没有基于时间维,而是汇集了工业界中普遍使用的信息安全工程实施方法。

(2) SSE-CMM 的评估方法必须得到标准化和得以公认,在 SSE-CMM 开发的过程中,SSE-CMM 的评定方法一直在同步发展(SSE-CMM 评定方法已经达到 2.0 版,于

1999 年 4 月 16 日发布)。

IA-CMM 自 2001 年提出以后发布了四个版本,最初被称为"信息安全评估(INFOSEC Assessment)能力成熟度模型",从 2003 年的版本开始改称"信息安全保障(INFOSEC Assurance)能力成熟度模型"。它产生的初衷源于美国国家安全局制定的一个信息安全保障培训和等级计划(INFOSEC Assurance Training and Rating Program, IATRP)。当时,美国国家安全局希望通过该计划,针对信息安全产业缺乏保证安全服务标准的问题,提供一种解决办法。随着 IA-CMM 由"信息安全评估"改名为"信息安全保障",IA-CMM 关注的领域得以拓宽,表明有关的工作侧重点已经不再局限在传统的"信息安全评估"的领域,而是开始关注信息安全保障能力成熟度及其测量。

IA-CMM 以 SSE-CMM 为基础,涉及信息安全保障分析过程,是不可裁剪的连续模型。这里,"不可裁剪"指的是,为一个给定的组织进行评价必须用到模型中所有的过程域。对信息安全保障进行分析需要依据某些具体的分析结果,例如,确定脆弱性,对策和威胁等。IA-CMM 关注的是产生这些结果的过程。

IA-CMM 确定了涉及信息安全保障活动的九个过程域。对于每个过程域,IA-CMM 定义了从 1 到 5 级的 5 个能力成熟度级别。随着能力成熟度级别的提高,组织通过连续执行的方式所建立的、到下一次评估前的评估过程的可信度也增强。

7.1.2 关于人员能力成熟度模型

同其他能力成熟度模型一样,P-CMM 的背景也是研究在软件生产中如何保证质量问题。它是卡内基梅隆大学在研究软件成熟度模型(SW-CMM)之后,为帮助组织的管理者改进人员的能力成熟度,不断提高员工劳动力能力而研究开发的能力成熟度模型。在这里,"劳动力能力"定义为一个机构执行其业务活动所需的员工知识、技能、处理能力的水平。

P-CMM 的产生与美国国防部有关。自 1980 年起,美国国防部每年大约花费 300 亿美元用于软件采购,延迟交货等因素影响了美国国防部的计划实施步骤。鉴于美国海军与空军当时已经借助 SW-CMM 成功地履行了合作协议,于是,美国国防部委托隶属于卡内基梅隆大学软件工程研究院的联邦基金研究与发展中心(Federally-Funded Research & Development Center, FFRDC)着手研究有关的问题,提供一种能够用来对技术人员的能力成熟度进行评价的方式。

1995 年,P-CMM 终于面世,一出现就成功地帮助一些大企业(例如,Ericsson、Boeing、Lockheed Martin、NovoNordiskIT、A/S,以及印度的 Tada Constancy Service)大幅地提升了企业员工的工作能力。后来,实际的应用情况表明,几乎各种类型的公司和组织机构都可以借助 P-CMM 来提高其员工的工作能力。

P-CMM 的基本原理可以概括为以下 10 条原则：

（1）在一个发展成熟的组织中，员工的劳动力能力直接关系到他们的业务业绩。

（2）组织的员工劳动力能力是该组织获得竞争和战略优势的来源之一。

（3）必须将员工的劳动力能力定义与组织的战略业务目标相关联。

（4）员工对于知识的渴望，将促使他们从仅关注具体工作元素的状态，转变到关注提高劳动力能力的状态。

（5）可以在个人、工作团队，劳动力能力和组织等多个层次，对员工的劳动力能力进行测量并加以改进。

（6）一个组织应该在改良劳动力能力方面进行投资，这种投资对提高组织业务的核心能力非常重要。

（7）组织在运营管理过程中要负责对员工的劳动力能力进行管理。

（8）可以将员工劳动力能力的进步，当作组织整体改进过程的组成部分，并在该过程中改进和提高劳动力能力。

（9）在员工个人获得他们的利益的同时，组织有责任为员工提供提高其能力的机会。

（10）因为技术在快速发展，组织的形式也在快速发展，组织必须对其员工劳动力进行持续地改进，并帮助员工获得的劳动力能力。

人员能力成熟度模型可以帮助组织进行的工作有：

（1）描述员工劳动力实践的成熟程度。

（2）指导建立和实施一个持续的劳动力发展计划。

（3）为组织当前的相关行动设定优先顺序。

（4）通过改进过程的方法对劳动力的发展进行整合。

（5）建立一个专业的、优秀的组织文化。

利用 P-CMM 实现上述作用的方法有两种：一是将 P-CMM 作为设定计划和依据该计划进行不断改进的一个行动指南，二是将 P-CMM 作为评估劳动力实践情况的标准之一。

P-CMM 之所以在国外得以风行，因为它允许组织自己按照自身状况定义人员能力成熟度级别。但是，P-CMM 也并非完美无瑕。它的缺点主要体现在四方面：

（1）过于注重细节和过程过于繁杂，琐碎，例如，模型自身的表述就长达上千页。

（2）由于具有系统化、全面化、专业性强的特点，作为一种商业行为的咨询服务而言，价格太高。

（3）在重视人力资源管理实践活动的同时，容易忽视与企业整体发展战略的匹配性，以及忽视人力资源战略本身。

（4）国情所致，对于中国企业而言，该体系中的部分标准和指标并不适用。

7.2 主要内容

7.21 模型的体系结构

人员能力成熟度模型的体系结构如图 7-2-1 所示。

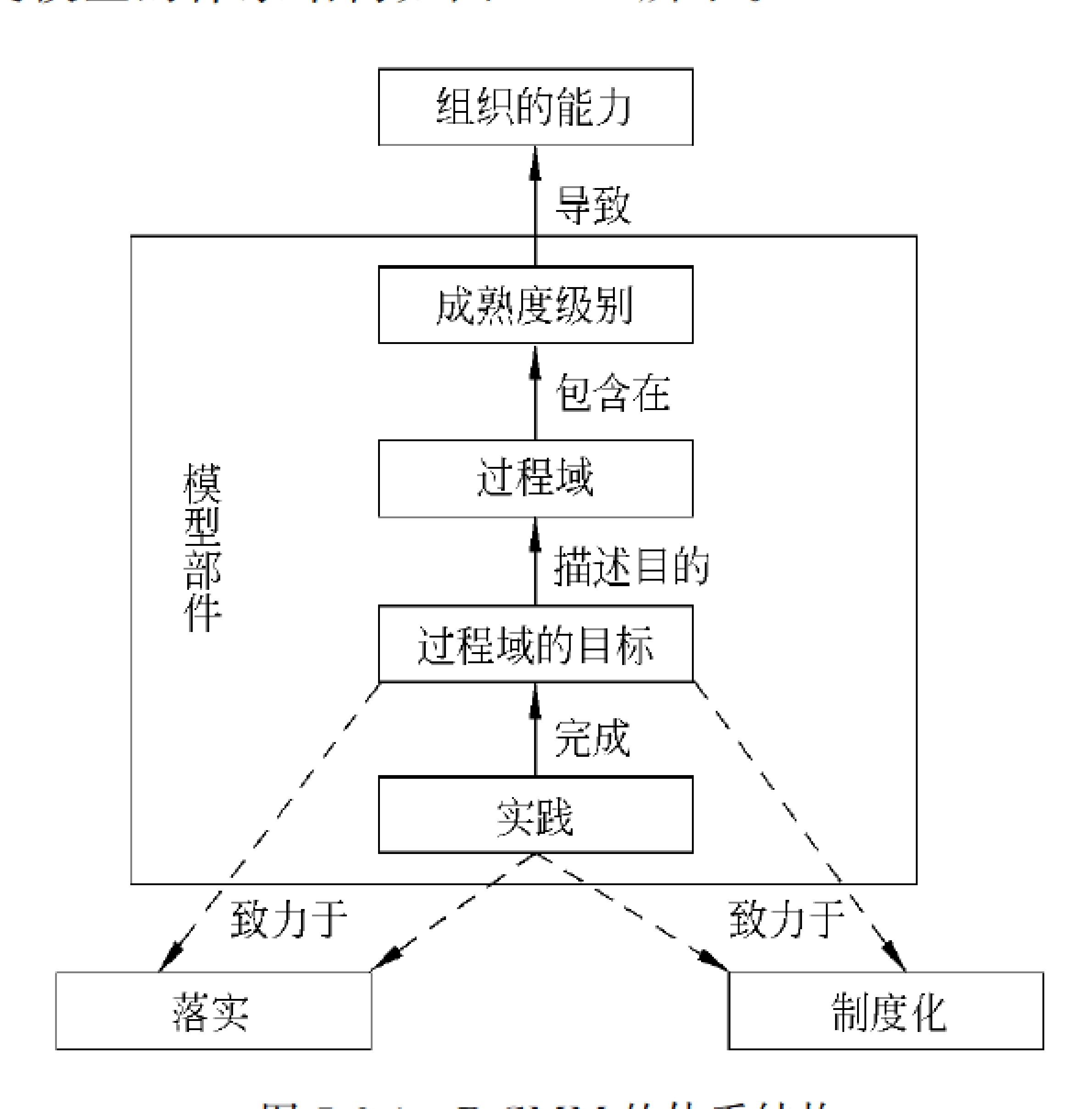


图 7-2-1　P-CMM 的体系结构

下面介绍模型部件中的四个组成部分。

(1) 成熟度级别(maturity levels):一个能力成熟度级别,表现了一个组织通过改进自身的一个或多个领域,所能够创建的新的能力水平。

(2) 过程域(process area):一个与上述改进活动相关的实践集合。在该集合中的元素全部被实践之后,即满足了一个目标集合后,可以达到某个成熟度水平,并促成能力增长。

(3) 目标(goals):通过实现过程域中的一系列实践,组织所能够达到的某种状态。

(4) 实践(practices):是一个过程域中的子过程,它促成达到这个过程域的目标。

可以将上述四个部分的关系简单地描述为:人员成熟度模型能够促进提高一个组织的能力,成熟度包含在需要处理的过程域中,为实现过程域需要提出一系列的目标,而达到这些目标则需要通过实践来完成,目标和实践都需要给予落实和制度化。

7.22 级别划分

人员能力成熟度模型将人员能力成熟度划分成 5 个级别，每个级别(第一级除外)都需要处理一些过程域(共有 22 个过程域)。

这 5 个级别是：初始级(initial level)、可管理级(managed level)、可定义级(defined level)、可预知级 (predictable level)、优化级 (optimizing level)。

(1) 在第一级(初始级)中，难以保留有才干的人员，虽然一些能力低下的组织总是抱怨员工能力不足，但是组织的行动并没有显示他们真正重视了这个问题。组织的管理者仅仅凭经验和感觉来进行管理。虽然这种管理工作可能也非常辛苦，但由于没有关注有关的全局性问题，经常造成员工责任不清，对员工疏于教育，员工只能够根据经验确定个人在组织中的定位，导致员工的行为存在以下四个特点：

① 在完成实践的过程中无法相互协调；

② 责任不到位；

③ 实践只是形式主义，没有实际效果；

④ 情绪不佳。

(2) 在第二级(可管理级)中，组织开始关注员工的个体行为。由于管理人员将改进劳动力能力作为最主要的工作任务，他们关注安置员工、协调责任、提供资源、管理表现、发展技能和针对员工成功的情况给予酬劳。这样的组织能够构建一个牢固的员工实践基础，从而帮助每一个有经验的员工从已有的劳动力能力水平提高到一个新的能力成熟度级别。

在此过程中，组织的管理者需要警惕员工个人发展可能遇到的各种问题，例如：超负荷工作，工作环境容易导致分心，得到的执行目标不明确或反馈信息不明确，缺乏有关的知识或技能，缺乏交流，士气低落。

第二级有六个过程域，分别是：

① 安置职工：目的是建立一个正式的方法，可以用它来调配工作，使该工作能够与新招募的、选拔的或调换分配的员工的才略和资格相匹配；

② 沟通和协调：目的是建立及时的、跨越部门机构的交流，保证员工能够共享信息和调整行动的有效性；

③ 操作环境：目的是建立并维持物理的工作条件，提供员工个人和员工团队有效完成工作需要的资源，保障员工工作精力集中；

④ 业绩管理：目的是建立对于员工工作业绩进行度量所需的目标，依据这些目标可以对员工的工作业绩进行讨论并持续提高业绩；

⑤ 培训和发展：目的是保证所有的员工具有完成工作需要的技能，并为员工提供发

展机会；

⑥ 报酬：目的是基于员工对组织的贡献和价值大小为其提供劳动报酬和利益。

这些过程域的关系如图 7-2-2 所示。

(3) 第三级(可定义级)有七个过程域，分别是：

① 能力分析：目的是识别执行组织的业务活动必需的知识、技能和处理才干，以便它们可能被发展成劳动力实践的基础；

② 劳动力计划：目的是用现在和未来的业务需要，在组织和员工个人这两个层次上协调劳动力的行为；

③ 能力发展：目的是坚持不懈地提高劳动力完成工作任务和履行职责的能力；

④ 事业发展：目的是保证为员工个人发展劳动能力提供机会，以使他们能够实现事业目标；

⑤ 基于能力的实践：目的是将所有劳动力实践建立在部分得到发展的劳动能力的基础上；

⑥ 工作团队发展：目的是围绕团队核心，组织员工进行工作；

⑦ 共享的文化：目的是保证将员工个人的知识纳入组织内部的信息流中并参与决策过程，同时得到员工对决策给予支持的承诺。

这些过程域的关系如图 7-2-3 所示。

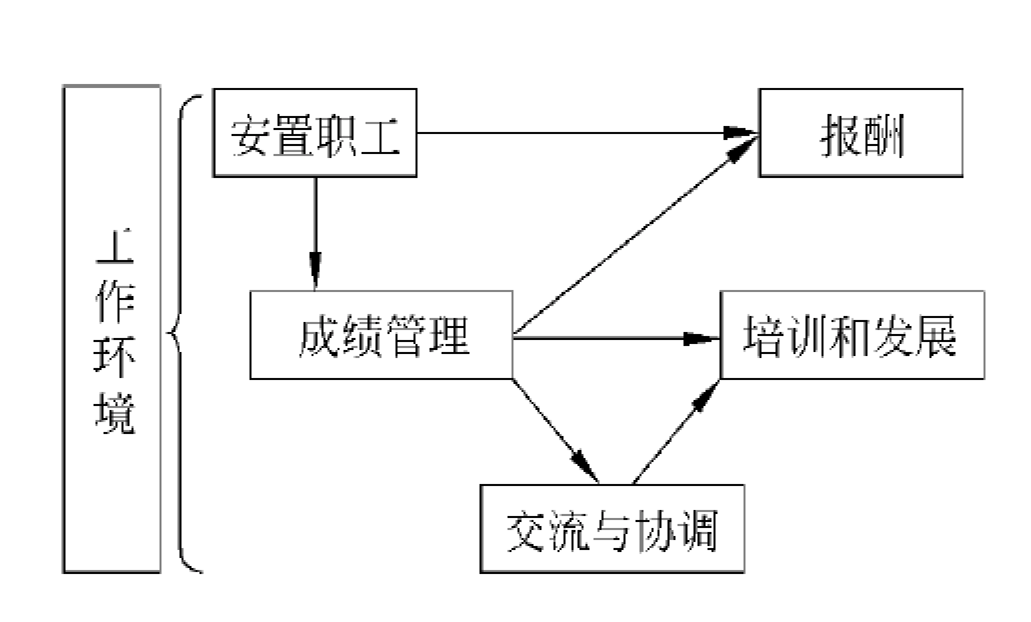


图 7-2-2 人员能力成熟度级别第二级中的过程域的关系

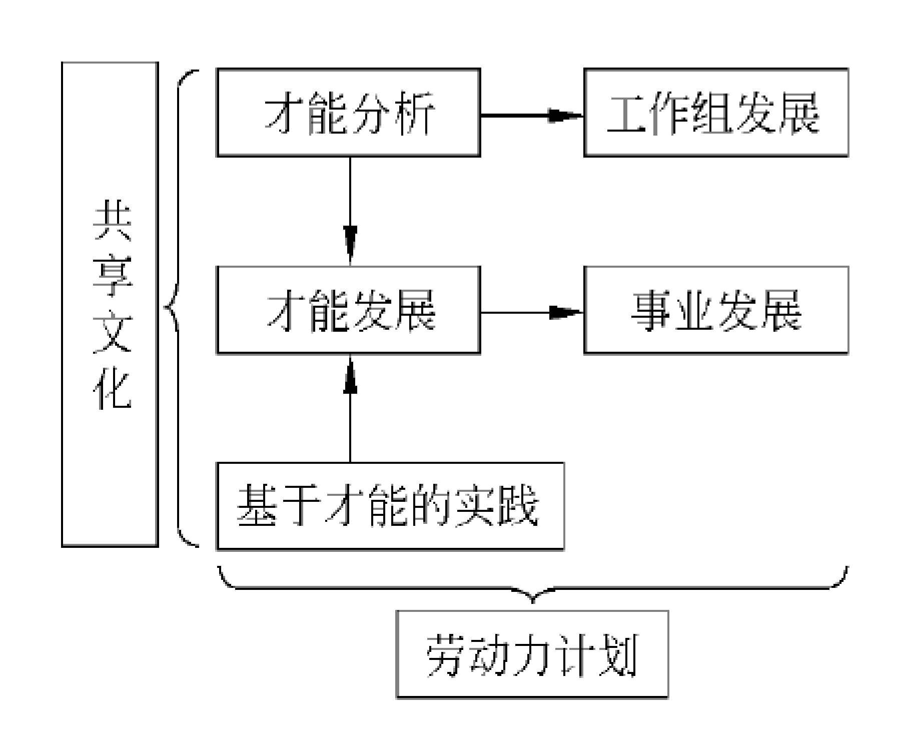


图 7-2-3 人员能力成熟度级别第三级中的过程域的关系

(4) 第四级(可预知级)有六个过程域，分别是：

① 能力整合：目的是借助整合不同的劳动力才能，改进相互依赖的工作效率和提高灵活性；

② 授权给工作团队：目的是为了最有效地实施团队的业务活动，将职责和权力授予工作团队；

③ 基于能力的资产：目的是在提高能力和业绩中采用基于能力的方法，赢得知识、经验和开发的工具；

④ 量化的业绩管理：目的是实现对业绩目标的可测度，预测和管理基于能力的过程；

⑤ 组织的能力管理：目的是量化并管理劳动力和他们执行的关键的、基于能力的过程；

⑥ 指导：目的是在员工中传递重要的经验教训，改进员工个人或工作团队的能力。

这些过程域的关系如图 7-2-4 所示。

(5) 第五级(优化级)有三个过程域，分别是：

① 持续的能力改进：目的是给员工个人和工作团队持续改进其能力提供一个基础；

② 组织业绩的调整：目的是用组织的业绩和业务目标，提高能够超越员工个人、工作团队和组织单一影响的业绩成效；

③ 持续的劳动力改进：目的是识别和评估经改良的或创新的劳动力实践和技术，并在组织中实现其中最有希望的一些成果。

这些过程域的关系如图 7-2-5 所示。

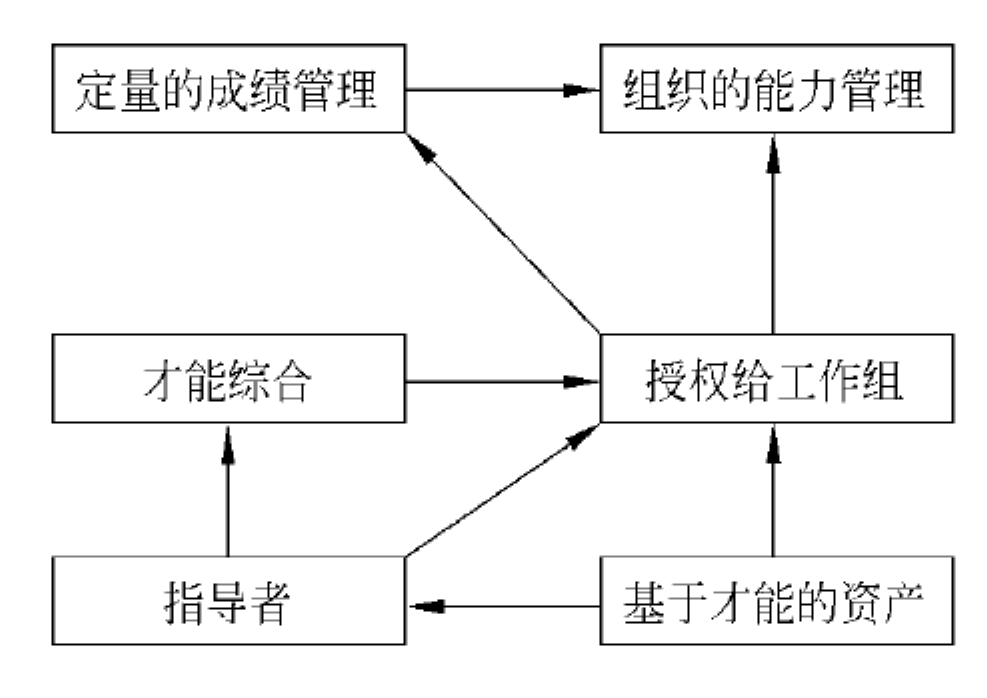


图 7-2-4　人员能力成熟度级别第四级中的过程域的关系

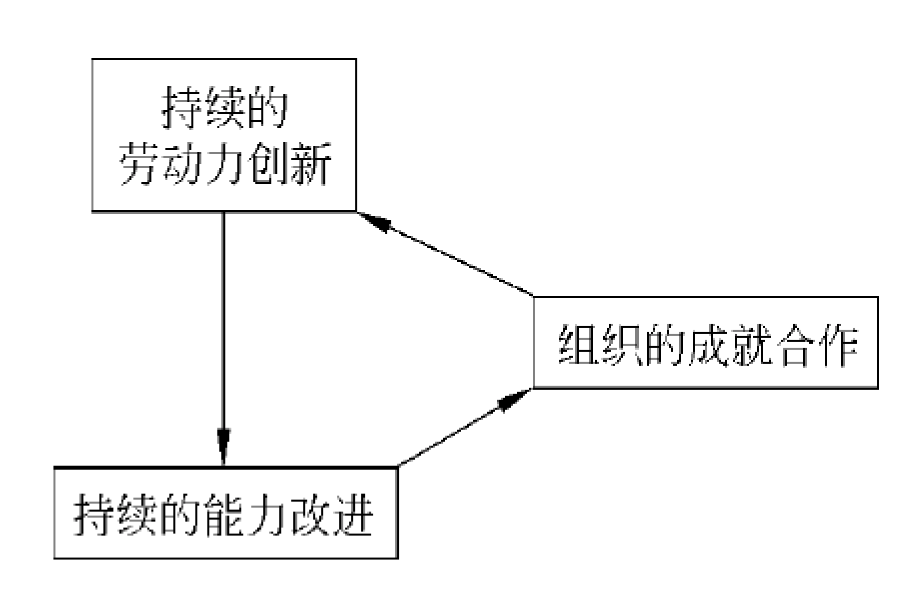


图 7-2-5　人员能力成熟度级别第五级中的过程域的关系

7.3　人员能力成熟度评价方法

P-CMM 评价方法是赫夫利(Hefley)研究了 3 年并于 1998 年提出的。这种方法描述了实现基于 P-CMM 的评价方法的技术和必要条件。它是一种诊断性的工具，可以支持、鼓励并使组织能够吸引、发展、激励、组织和保持人才，而正是这些人才能够使组织能够稳步提高整体能力。这种方法通过发现组织在人员管理方面的优势和弱势，帮助组织管理

者清楚地洞察其人员能力。在明确了组织的经营目标和现有的人员能力成熟度水平后，这种评价方法关注的重点是如何确定改进措施并实施。

标准的 P-CMM 评价方法分为以下四个阶段：

(1) 准备阶段——为评价做准备。

(2) 问卷调查阶段——实施人员管理调查。

(3) 评价阶段——实施现场评价。

(4) 报告阶段——报告评价结果。

上述每一个评价阶段都包括了各种各样的任务。虽然四个阶段是前后连续的，但各阶段包含的任务却有重合之处。

只有得到授权的 P-CMM 评价专家才能主持正式的 P-CMM 评价。评价小组包括一名经卡内基梅隆大学软件工程研究院授权的 P-CMM 评价专家，和一些经过 P-CMM 培训的组员，一般不超过 8 人。只有小组成员才能评价问卷的反馈情况、检查文件、实施评价面谈、整理评价数据，和确定成熟度等级。

评价小组必须具备以下的素质和资格：至少有一人必须是卡内基梅隆大学软件工程研究院授权的 P-CMM 评价专家，至少有一人来自被评价的组织，至少有一人有全面丰富的人力资源管理经验，所有组员都必须具备进行评价所需的知识、技术和能力，并且经过 P-CMM 培训。

在“评价—改进—再评价—再改进”的循环过程中，组织不断提高其人员管理水平，从而提高其人员成熟度。

当 P-CMM 评估和软件过程评估一起进行时，P-CMM 的评估数据必须单独收集，因为它的评估单元并不是软件过程评估的实施单元——项目，而是组织的人事单元，比如工作组、部门以及这些单元如何实施劳动力实践。尽管这样，P-CMM 评估还是可以使用软件过程评估的一些惯例，例如培训评估队伍、收集问卷数据、确认数据可信度以及对组织不同级别的人员进行访谈等。P-CMM 的评估结果可以和别的评估结果同时得到，但是必须另外进行单独的分析。

P-CMM 评估工作将劳动力实践视为在全组织内进行的工作。P-CMM 评估组会判断相应的实践活动是否确实在全组织内得以实施，以及这种实施情况是否得以制度化。它们还会判断每个关键过程域的目标和意图是否已经实现。当然，它们没有必要评估超过当前组织成熟度等级的过程域。

P-CMM 评估的结果勾勒了组织在 P-CMM 过程域上所表现出来的强弱程度。一个组织的成熟度级别就是组织实现的所有关键过程域中的最低级别。

7.4 小结

本章介绍了人员能力成熟度模型的产生背景、主要内容和人员能力成熟度评价方法，重点介绍了人员能力成熟度模型五个级别中的具体过程域，以及处在同一级别中的各个过程域彼此间的联系。为了帮助读者理解人员能力成熟度模型的概念和作用，我们简要回顾了能力成熟度模型研究活动的最初起源，以及美国卡内基梅隆大学的一系列研究活动，希望能够在此基础上说明人员能力成熟度模型与其他若干个更为大家所熟知的能力成熟度模型(例如 SSE-CMM、IA-CMM、SE-CMM)的联系和区别。最后，我们介绍了人员能力成熟度评价方法的主要思想，以及该评价方法在具体评估实施过程中需要注意的一些问题，希望帮助读者进一步理解人员能力成熟度模型及其应用模式。

习　题

1. 什么是 CMM？它的作用是什么？
2. 什么是 SSE-CMM？它有哪些特点？
3. IA-CMM 与 SSE-CMM 有什么联系？
4. P-CMM 和 CMM 有什么关系？为什么要在出现了众多的 CMM 之后还要发布 P-CMM？
5. P-CMM 可以分为几个组成部分？各部分之间的关系如何？
6. P-CMM 的五个成熟度级别之间的差别在何处？
7. P-CMM 和第 6 章提到的 SSE-CMM 有何差异？

第 8 章 案例研究

8.1 案例一：某艺术馆网络安全解决方案研究

某艺术馆占地面积约 $4000m^2$，有 $1800m^2$ 的展览场地。该馆的局域网络由 Accton 智邦大陆科技有限公司设计和安装。

经过充分考虑和反复论证，在该馆有关人员的协助下，智邦科技公司将用户的需求定位在以下 4 点：

（1）设置三个无线区域，即办公区域（VLAN-1）、公共用户区域（VLAN-2）、公共接入区域（VLAN-3）。办公区域和公共用户区域的用户都能接入到公共接入区域，公共开放用户通过无线上网，免费享受 Internet 服务。用户之间相互隔离，并且与办公区域隔离，即数据不能共享。

（2）启用最高等级的无线加密方式，保证艺术馆内部网络不被侵入。

（3）员工宿舍与主楼之间启动 VPN 方式进行连接，实现远程连接。

（4）办公用户能共享上网，共享打印机，共享服务器文件资源。

依据上述需求定位，解决方案实施后的网络拓扑图如图 8-1-1 所示。

其中，方案设计者使用了一台 SMC6726AL2 24 口网管交换机连接用户计算机、服务器等，其中服务器连接有一系列打印机，提供打印服务。网络中有 3 个 VLAN 网络，VLAN-1 为办公区域，VLAN-2 为公共用户区，VLAN-3 为公共接入区。该网络能够支持无线应用，为办公人员和公共用户提供无线上网服务，例如，用户可以使用配有无线网卡的笔记本、PDA/Packet PC 等无线设备接入本网络享受上网服务。VLAN-3 公共接入区通过 SMCBR14VPN 路由器与 Internet 相连，在该路由器上配置有 SPI 防火墙、内置 NAT 和 DHCP 服务。

方案设计者提供的资料显示，SMCBR14VPN 路由器部署在艺术馆主楼旁的员工宿舍（附楼），可以同时启动 40 个独立的 IPSec VPN 通道，可以对分支机构和出差在外的移动工作人员与本网络的连接进行保护，并且提供了 DMZ 功能，可以根据需要在 DMZ 区

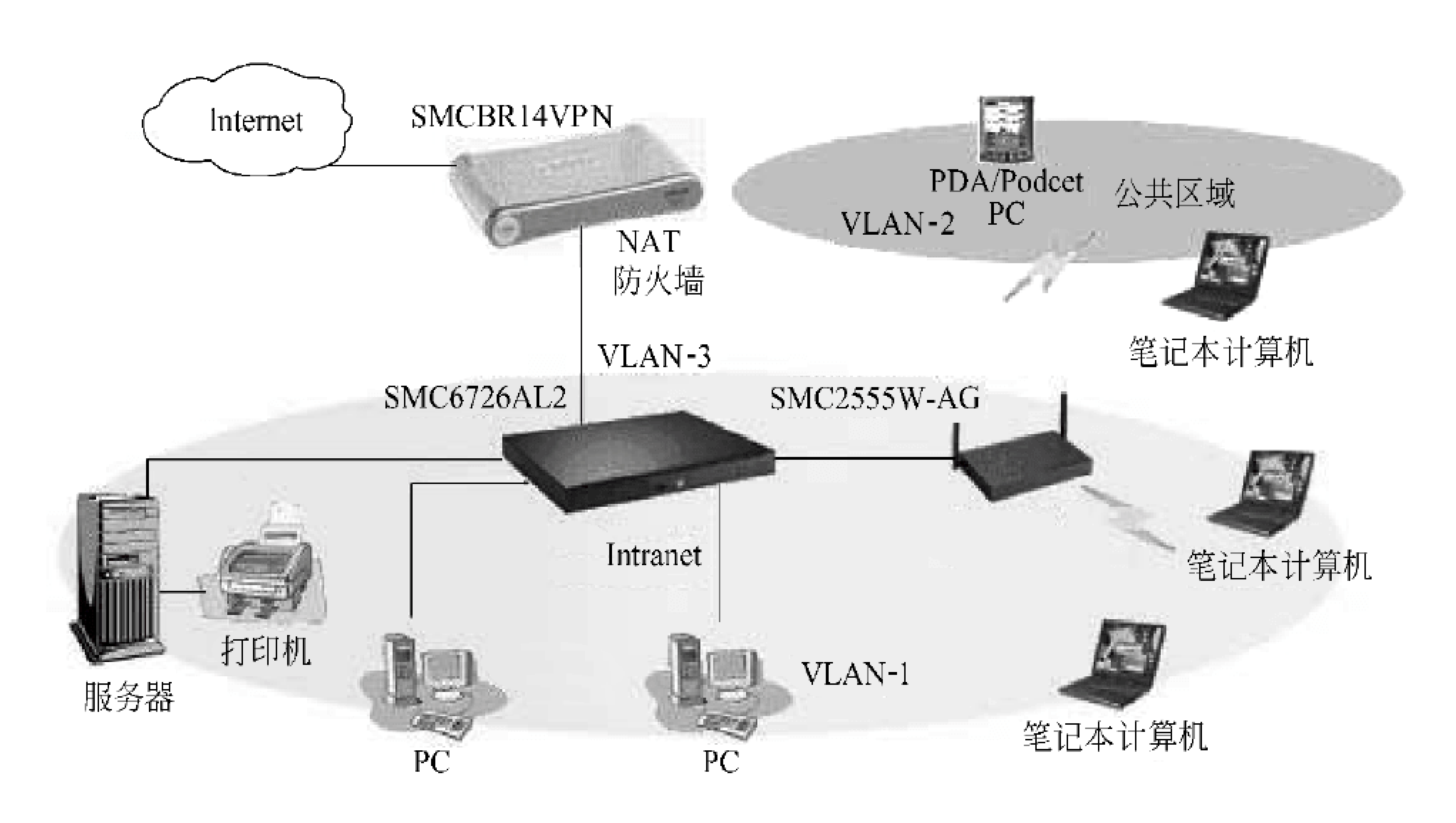


图 8-1-1　解决方案实施后的网络拓扑图

域内部署 Web 服务器。

对于上述解决方案的安全性，分析研究结果如下：

首先，对于无线服务的策略，考虑到艺术馆的面积并不是非常大，若采用两台 AP 的话可能会引起信号的重叠干扰，而且造成设备重复安置的浪费。设计者采用了一台 AP 两套 SSID 的策略，使用了 SMC 企业级无线网桥/AP-SMC2555W-AG，此款设备的高级设置中可以允许用户在一台 AP 上，同时公布出两个 SSID，并且两个 SSID 分属两个 VLAN。

一个 SSID 用来公布给公共用户，公共用户连接这个 SSID 后，自动加入 VLAN-2，且启用无线用户相互之间隔离功能，这样做有效防止了公共用户间计算机病毒的相互感染。

另一个 SSID 关闭广播功能，只告知内部办公人员，工作人员连接这个 SSID 后，自动加入 VLAN-1，为进一步增强内部办公无线网络的安全性，对内部使用无线网络的用户启用 128 位的 WPA-PSK 方式的加密。

但是这样做仍然有一个潜在的危险，就是工作人员可能会泄露后一个 SSID，而使得攻击者有机可乘。攻击者一旦得到了这个 SSID 地址，可以利用无线网络的开放性特点，暗中对其进行监听而不会被发现，当攻击者收集到足够的信息以后，就有可能实施攻入行为。所以，建议当连入办公 SSID 以后，不是直接加入 VLAN-1，而是先对身份进行验证，才允许登录。例如，可以附加 MAC 限制，使用账号口令，或者采用生物特征识别等技术，对内部人员的登录进行控制等。

对于 VLAN-1，为办公网络，设计者在路由器上设置了 VLAN-1 和 VLAN-2 不能互访，这种隔离增强了其安全性，VLAN-2 中出现问题，并不影响 VLAN-1，反之亦然。但

是，由于这部分网络中有服务器存在，其安全问题仍不容忽视。

由于 VLAN-1 仍可通过 VLAN-3 与 Internet 相接，容易感染 Internet 上的病毒，同时，VLAN-1 中的工作人员的操作也影响了这部分网络的安全，如工作人员接受带病毒的邮件、运行了带病毒的程序，使用了带病毒的外存储介质（光盘、优盘等），病毒的感染不仅可能会使服务器停止服务影响工作，甚至可能造成整个局域网的瘫痪。

因此，必须对 VLAN-1 中的各个机器加装杀毒软件，定期查杀、定时升级，而且要有专人对服务器进行维护，一旦出现问题要及时补救。还要对工作人员的上机工作做出要求，最好对所有工作人员进行一些安全常识的培训，并给出安全责任的条例，对工作人员的私人行为做出警告。如有必要需要对网络的某些服务做出禁止，提供本地的邮件服务以便对电子邮件的病毒传播进行控制。

对于 VLAN-3，这里是整个局域网与 Internet 的接口，其安全的重要性不言而喻，从资料中可知路由器配内置有 SPI 防火墙，但是并没有给出其防火墙的资料，由于现今能够穿过防火墙的病毒和攻击方法很多，因此这里的防火墙可靠与否也是一个很大的问题，必须对它进行正确配置，并且有专人对其进行实时监视。特别地，如果局域网内部署了 Web 服务器，整个局域网会暴露在 Internet 下，会有更多的恶意攻击发生，因此，保证防火墙的可靠性，及时发觉入侵活动并做出处理，非常的重要。

考虑到这个网络的规模确实不大，而且考虑其为一个公益性机构的艺术馆，加之还未提供 Web 服务，恶意攻击者应该为数不多，但是未雨绸缪，安全措施还是一定要做好的，将来一旦推出了 Web 服务，有必要对网络拓扑进行一些调整，再分出一个独立的区域放置 Web 服务器，如果需要 Web 服务器与现存服务器的连接，最好在 Web 服务器与现存服务器中间加一个中介进行防护，并对通信进行加密。

8.2 案例二：某市政管理委员会网络安全解决方案研究

在当今全球一体化的商业环境中，信息的重要性被广泛接受，信息系统在商业和政府组织中得到了真正的广泛的应用。许多组织对其信息系统不断增长的依赖性，加上在信息系统上运作业务的风险、收益和机会，使得信息安全管理成为企业管理越来越关键的一部分。管理高层需要确保信息技术适应企业战略，企业战略也恰当利用信息技术的优势。

某市政管理委员会原有网络拓扑图如图 8-2-1 所示。网络中内部 OA 服务器局域网和内部办公局域网及外部服务器局域网相互逻辑隔离。在内部 OA 服务器局域网中接入

内网 OA 系统的 Web 服务器和数据库服务器,在外部服务器局域网接入外网 Web 服务器、数据库服务器、DNS/E-mail 服务器,办公局域网中的终端可以访问内网 OA 系统的同时也可以访问 Internet,内网 OA 服务器和外网服务器之间也可以实时通信,三网通过两台防火墙进行访问控制以达到逻辑隔离的效果。

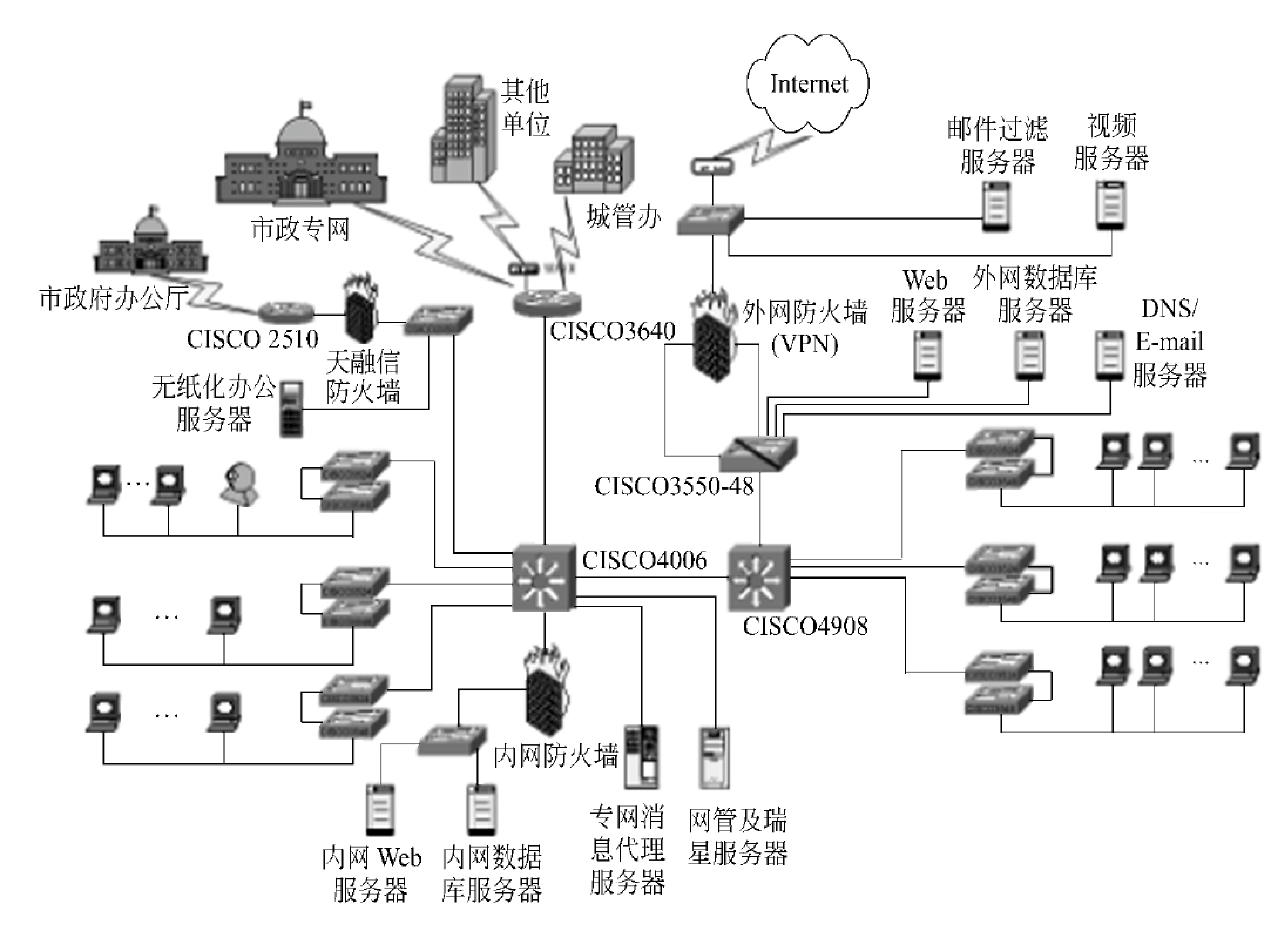


图 8-2-1 某市政管理委员会原有网络拓扑图

该市级城市管理信息平台的网络系统逻辑结构如图 8-2-2 所示。

这个信息系统面临的安全性问题,主要来源于以下风险要素:

1) 环境和硬件

地震、水灾、火灾、有害气体和其他环境事故(如电磁污染等)的破坏。

2) 网络层

网络层是网络入侵者进攻信息系统的渠道和通路。许多安全问题都集中体现在网络层的安全方面。其具体表现如下:

(1) 网络拓扑结构:保证网络安全的首要问题就是要合理划分网段,利用网络中间设备的安全机制控制各网络间的访问。

(2) 网络协议:由于网络系统内运行的 TCP/IP 协议并非专为安全通信而设计,所以

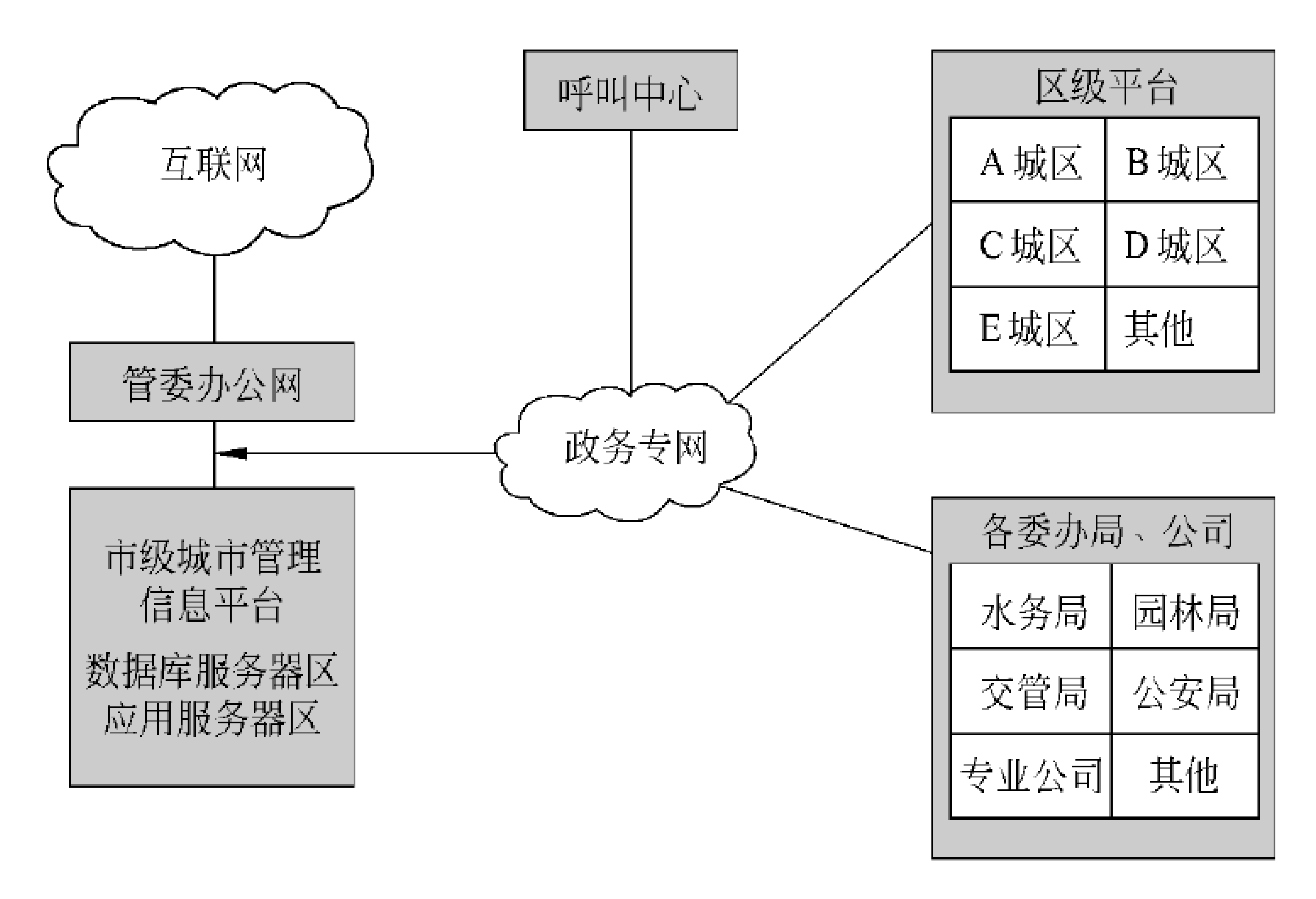


图 8-2-2　某市级城市管理信息平台的网络系统逻辑结构图

网络系统存在大量安全隐患和威胁。

3）操作系统

由于目前所使用的计算机网络操作系统，其系统本身在结构和代码设计时偏重于考虑系统使用的方便性，所以易导致系统的安全机制不健全，存在很多安全漏洞。

4）数据库

由于数据库管理系统对数据库管理是建立在分级管理的概念上，因此数据库管理系统的安全问题也是可想而知。再则数据库管理系统的安全必须与操作系统的安全相配套，所以随之而来就带来了一系列的问题，这无疑是一个先天的不足。

5）应用系统

应用层安全是指网络上的应用系统的安全，包括各个业务系统的应用系统，例如内部办公自动化系统、网上审批系统等。

应用层安全的解决目前往往依赖于网络层、操作系统、数据库的安全，由于应用系统复杂多样，没有特定的安全技术能够完全解决一些特殊应用系统的安全问题。但对一些通用的应用程序，如 WebServer 程序、FTP 服务程序、E-mail 服务程序、浏览器、MS Office 办公软件等，漏洞扫描系统可以帮助检查这些应用程序自身的安全漏洞和由于配置不当造成的安全漏洞。

6）人为因素

无论什么样的网络系统都离不开人的管理，但大多数网络系统又缺少安全管理员，特别是高素质的网络管理员。另外，也缺少网络安全管理的技术规范，缺少定期的安全测试

与检查以及缺少安全监控。甚至有的网络管理员和用户的注册、口令等至今还处于默认状态。所以人为因素也是影响信息系统安全的一个重要原因。

如图 8-2-3 所示，市级城市管理信息平台的网络系统面临的威胁种类各异，主要有以下几类：

（1）内部窃密。

（2）截收。

（3）非法访问。

（4）破坏信息的完整性。

（5）冒充。

（6）破坏系统的可用性。

（7）重放。

（8）否认。

（9）其他威胁。

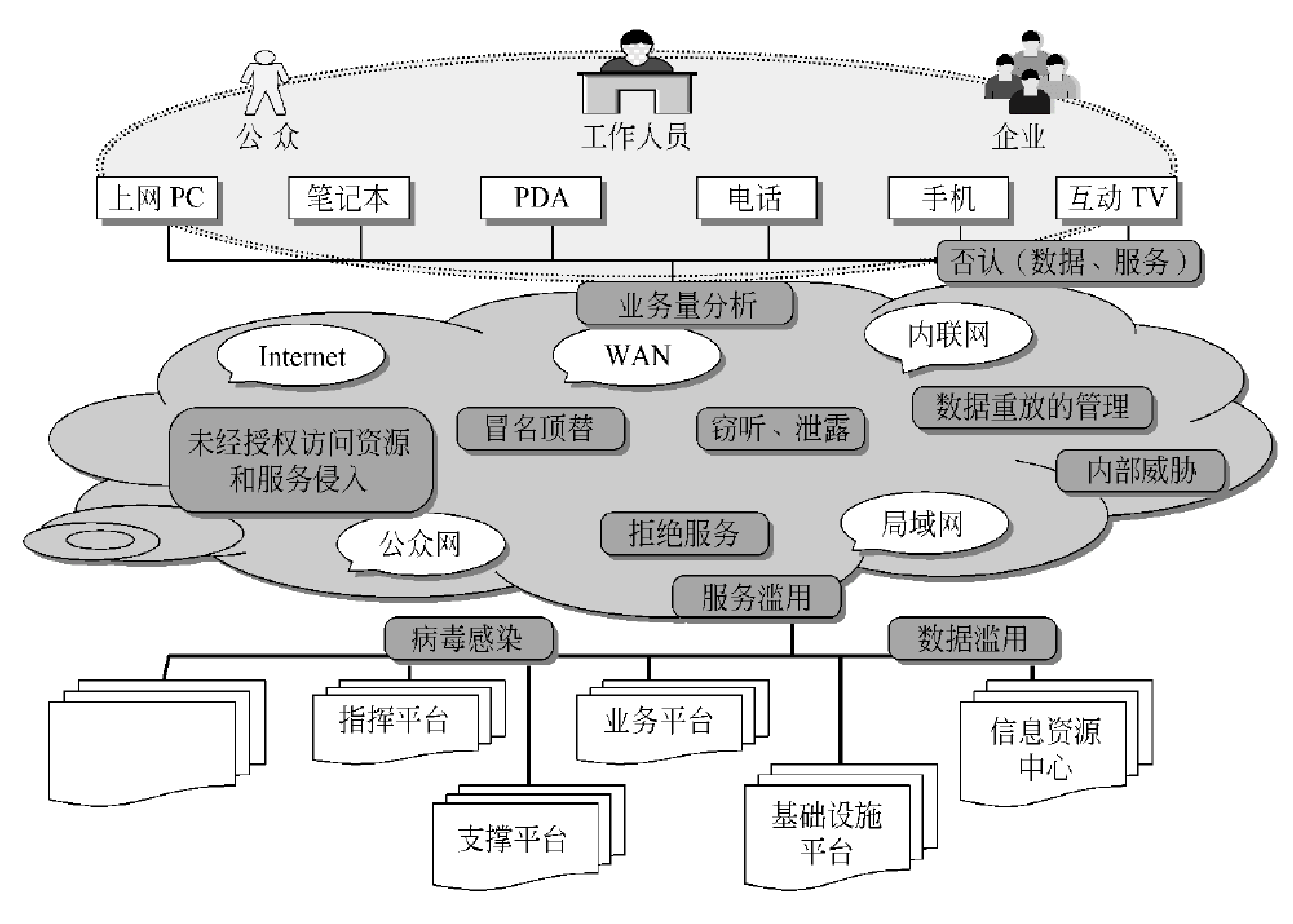


图 8-2-3　某市政管委信息化网络系统各构成要素的安全风险

这些威胁可能存在的位置、安全风险以及对应的安全需求见表 8-2-1。

表 8-2-1 某市级城市管理信息平台的网络系统面临的安全风险和安全需求

位 置	安 全 风 险	安 全 需 求
互联网出口	基 础 设 施	
	病毒和主动攻击	保证网络设备不被入侵
	信息窃取，假冒，否认	保证边界路由和协议的安全
	信息安全访问的问题	能够与攻击源追踪系统互通
	网络可靠性问题	保证不应降低接入速度和增加显著延迟
管委办公网	接 入 设 备	
	对设备的控制企图	保护设备安全
	通过边界设备发起对其他网络的攻击	限制进入网络的非法数据包
		记录和跟踪非法数据包来源
	前 端 服 务	
	DoS 攻击	防御 DoS
	系统本身的缺陷	保护服务提供设备的安全(操作系统)
		保护服务软件系统的安全
	信息窃取，假冒，否认	保护服务系统数据的安全
		与互联网隔离
		实时入侵告警和响应
政务专网	核心网络设备	
	网络设备的企图控制	保证网络设备不被入侵
	针对路由协议的攻击	保证路由协议的安全
	针对其他服务协议的攻击	保证服务协议的安全
		保证不过多地降低系统性能
	呼叫中心接入政务专网	和政务专网隔离
	市级平台接入政务专网	和政务专网隔离
	区级平台接入政务专网	和政务专网隔离
	委办局和专业公司接入政务专网	和政务专网隔离

续表

位　　置	安 全 风 险	安 全 需 求
政务专网	数 据 交 换	
	传输数据的截获和修改	保护提供管理监控功能的设备
	存储数据的修改和破坏	敏感数据的传输加密和完整性检查
市级平台专网	应用服务器区	
	内部攻击	严格的访问控制
	渗透到网络中心后，发起攻击	对系统和数据访问的审计
	传输数据的截获和修改	保护提供管理监控功能的设备
	存储数据的修改和破坏	敏感数据的传输加密和完整性检查
		敏感数据的存储/备份加密
		系统/数据的备份和恢复
		和办公网隔离
		实时入侵告警和响应
	数 据 库 区	
	内部攻击	严格的访问控制
	渗透到网络中心后，发起攻击	对系统和数据访问的审计
	传输数据的截获和修改	保护提供业务支持的设备
	存储数据的修改和破坏	敏感数据的传输加密和完整性检查
		敏感数据的存储/备份加密
		系统/数据的备份和恢复
		和应用服务器区隔离
		实时入侵告警和响应

8.3 小结

本章介绍了两个案例，分别是某艺术馆网络安全解决方案和某市政管理委员会网络安全解决方案。我们对每个案例中提到的技术和管理解决方案都进行了分析。其中，对于案例一，侧重分析无线网络应用的安全问题。对于案例二，侧重分析政务网络的信息安

全隐患与需求。

我们期望通过这两个案例帮助读者在了解和掌握本书前述各章内容的基础上，能够尝试着解决客观世界中的现实问题，通过采取必要的技术方法和管理措施，改善网络与信息系统的安全状况，学以致用。

习　题

1. 结合案例一考虑以下问题：

(1) 将该网络划分为三个虚拟专网(VLAN)的作用是什么？

(2) 为何在解决方案中采用了一台 AP 两套 SSID 的策略？

(3) 描述该方案所用无线加密设备的主要功能。

(4) 如果随着业务的拓展，需要对该艺术馆的网络拓扑进行一些调整，分出一个独立的区域放置 Web 服务器等设备，画出必要的示意图，并说明图中主要组件的作用。

2. 结合案例二考虑以下问题：

(1) 该市政管委信息化网络系统中的主要信息安全风险有哪些？

(2) 核心网络设备、应用服务器和数据库的主要信息安全需求包括哪些？

(3) 需要采用什么技术来满足该网络的安全需求？请列出必要的 4～6 个产品名单，并说明这些产品的主要功能、性能指标和配置特点。

(4) 如何改进信息安全管理？

附录 A

图 表 目 录

附录B

缩 略 语

英文缩写	英文全称	中文翻译
ADM	Architecture Development Method	体系结构开发方法
ADML	Architecture Development Method Language	体系结构描述标记语言
AES	Advanced Encryption Standard	高级加密标准
AP	Access Point	无线接入点
ATM	Asynchronous Transfer Mode	异步传输模式
CDSA	Common Data Security Architecture	通用数据安全体系结构
CE	Certified Execution	认证执行
CFCA	China Financial Certification Authority	中国金融认证中心
CMM	Capability Maturity Model	能力成熟度模型
CORBA	Common Object Request Broker Architecture	公共对象请求代理体系结构
CPI	Crypt Provider Interface	密码服务系统接口
C/S	Client/Service	客户机/服务器
CSSM	Common Security Service Manager	通用安全服务管理器
DDN	Digital Data Network	数字数据网
DGSA	Defense Goal Security Architecture	目标安全体系结构
DISA	Defense Information Systems Agency	美国信息系统防卫局
DISSP	Defense Information System Security Program	美国国防部信息系统安全计划
DMZ	Demilitarized Zone	停火区
DOTS	Defense Overall Transition Strategy	国防部总体过渡策略
DSL	Digital Subscriber Line	数字用户线路
EA	Enterprise Architecture	企业体系结构
EAP	Extensible Authentication Protocol	可扩展认证协议
ECMA	European Computer Manufactory Association	欧洲计算机制造商协会
EIA	Electronic Industry Association	电子工业协会
ESSID	Extended Service Set Identifier	扩展服务区标识符
FCC	Federal Communication Commission	美国联邦通信委员会
FIPS	Federal Information Process Standard	美国联邦信息处理标准
FTP	File Transfer Protocol	文件传输协议

英文缩写	英文全称	中文翻译
GUI	Graphical User Interface	图形用户界面
HIPS	Host Intrusion Protection System	主机入侵防御系统
IA-CMM	INFOSEC Assessment Capability Maturity Model	信息安全评估能力成熟度模型
IATRP	INFOSEC Assurance Training and Rating Program	信息安全保障培训和等级计划
IAL	Intel Architecture Labs	Intel 体系结构实验室
IATF	Information Assurance Technology Framework	信息保障技术框架
ICMP	Internet Control Message Protocol	Internet 控制消息协议
IDES	Intrusion Detection Expert System	入侵检测专家系统
IDS	Intrusion Detection System	入侵检测系统
IKE	Internet Key Exchange	Internet 密钥交换协议
IP	Internet Protocol	Internet 协议
IPSec	Internet Protocol Security	Internet 协议安全
ISDN	Integrated Service Digital NeTwork	综合业务数字网
ISO	International Organization for Standardization	国际标准化组织
ISMS	Information Security Management System	信息安全管理体系
KMI	Key Management Infrastructure	密钥管理基础设施
L2TP	Layer 2 Tunneling Protocol	第二层隧道协议
MIB	Management Information Base	管理信息库
NGSCB	Next Generation Secure Computing Base	下一代安全计算基础
NIC	Network Interface Card	网络接口卡
NIST	National Institute of Standards and Technology	美国国家技术标准局
OSI	Open System Interconnect	开放系统互连
P-CMM	People CMM	人员能力成熟度模型
PDCA	Plan-Do-Check-Act	规划—实施—检查—处置
PDRR	Protection-Detection-Reaction-Restore	保护—检测—响应—恢复
PDP	Policy Decision Point	策略决策点
PEPs	Policy Enforcement Points	策略实施点
PMI	Privilege Management Infrastructure	授权体系
PP2P	Point to Point Tunneling Protocol	点对点隧道协议
PPP	Point to Point Protocol	点到点协议
PKI	Public Key Infrastructure	公钥基础设施
RIP	Routing Information Protocol	路由信息协议
SMDS	Switched Multimegabit Data Service	可交换多兆位数据服务
SNMP	Simple Network Management Protocol	简单网络管理协议
SPI	Service Provider Inferface	服务提供接口

英文缩写	英文全称	中文翻译
SSE-CMM	Systems Security Engineering Capability Maturity Model	系统安全工程—能力成熟度模型
SW-CMM	Software Capability Maturity Model	软件能力成熟度模型
TAFIM	Technical Architecture Framework of Information Management	信息管理技术体系结构框架
TCG	Trusted Computing Group	可信计算组织
TCP	Trusted Computing Platforms	可信计算平台
TIA	Communication Industry Association	通信工业协会
TOGAF	Technical Open Group Architecture Framework	开放组织体系结构框架
TPM	Trusted Platform Module	可信平台模块
XDSF	X Distributed System Framework	分布式系统安全框架
XOM	Execute-only Memory	仅执行内存
VLAN	Virtual Local Araa Network	虚拟局域网
VPN	Virtual Private Network	虚拟专用网
WAE	Wireless Application Environment	无线应用环境
WAN	Wide Area Network	广域网
WDP	Wireless Data Protocol	无线数据报协议
WEP	Wired Equivalent Privacy	有线等效保密
WIM	Wireless Identifier Module	无线身份识别模块
WLAN	Wireless Local Area Network	无线局域网
WPA	Wi-Fi Protected Access	Wi-Fi 保护访问
WPKI	Wireless Public Key Infrastructure	无线公钥基础设施
WSP	Wireless Session Protocol	无线会话协议
WTLS	Wireless Transport Layer Security	无线传输层安全

参 考 文 献

1 U. S Department of Defense. Technical architecture for information management. volume 1:Overview, 1996

2 U. S Department of Defense. Technical architecture for information management. volume 6: DoD Goal Security Architecture, 1996

3 Ahmed P. Security Management for OSI Networks. Computer Communications, 1994, 17(7): 544～553

4 Jay Ramachandram. Design Security Architecture Solutions. John Wiley&Sons, 2002

5 Bellovin S. Report of the IAB Security Architecture Workshop. RFC2316, 1998

6 Bell D E, LaPadula I J. Secure Computer System: Unified Exposition and Multics Interpretation. MITRE Corporation, MTR-2997, 1976

7 John W Satzinger, Robert B Jackson, Stephen D Burd. Systems Analysis and Design in a Changing World. 2000

8 Anthony B. Specification and Validation of a Security policy Model, IEEE Transactions on Software Engineering, 1995, 21(2)

9 Cheh G. Policy Management Requirements. HP Lab Bristol, HPL-98-64, April, 1998

10 Clark D, Wilson D. A Comparison of Commercial and Military Security policies. Proceedings of IEEE Symp. on Security and Privacy, Los Alamitos, USA, 1987

11 Denning D E. A lattice model of Secure Information flow, Communications of the ACM, 1976, 19(5):236～243

12 DoD. Trusted Computer Systems Evaluation Criteria (TCSEC). US DoD 5200. 28-STD, 1985

13 Haixin D, Jianping W. Security Management for Large Computer Networks. the 5th Asia Pacific Communication Conference(APCC'99), Beijing: 1999, 256～261

14 Gasser M, Goldstein A, Kaufman C, et al. The Digital Distributed System Security Architecture. In Proceedings of the 12th national Computer Security Conference, Baltimore, MD. 1989. 305～319

15 International Standards Organization. Information Proceeding Systems-OSI RM. Part 2: Security Architecture. ISO. TC 97 7498-2, 1988

16 Kent S. Security Architecture for the Internet protocol. RFC2401, 1998

17 Kohl J, Neuman C. The Kerberos Network Authentication Service V5, RFC1510, 1993

18 Kaijser N, Parker T, pinkas D. SESAME: The Solution to Security for Open Distributed Systems. Computer Communications, 17(7):501～518, 1994

19 Edward A. Feustel, Terry Mayfield. The DGSA: unmet Information Security Challenges for Operating System Designers. ACM Operating Systems Review, vol. 32, No. 1, Jan1998, 3～22

20 GB 17859—1999,计算机信息系统安全保护等级划分准则. 中国国家质量技术监督局, 2001

21 Matt Bishop. Computer Security:Art and Science,Addison-Wesley,2004
22 http://www.nsc.org.cn/disp_article.asp? AE_ACID=477
23 http://www.e-works.net.cn/ewk2004/ewkArticles/478/Article361.htm
24 http://www.tc260.org.cn:7080/sy/xwzt/htmls/20040513000002.html
25 http://www.topsec.com.cn
26 http://www.venustech.com.cn
27 http://www.kill.com.cn
28 http://www.cfca.com.cn
29 http://www.sei.cmu.edu
30 http://csoonline.com.cn/blogs/lovelife/archive/2006/08/12/1437.aspx
31 http://blog.edu.cn/user1/6542/archives/2007/1688293.shtml
32 http://www.nercis.com.cn/standardv.jsp? id=66
33 http://www.nercis.com.cn/laws.jsp
34 张晓伟等编著.信息安全策略与机制.北京：机械工业出版社,2004
35 Barman S 著.编写信息安全策略.段海新.刘彤译.北京：人民邮电出版社,2002
36 国家信息安全工程技术研究中心,国家信息安全基础设施研究中心编著.电子政务总体设计与技术实现.北京：电子工业出版社,2003
37 http://www.27000.org
38 http://www.iso.org

读者意见反馈

亲爱的读者：

感谢您一直以来对清华版计算机教材的支持和爱护。为了今后为您提供更优秀的教材，请您抽出宝贵的时间来填写下面的意见反馈表，以便我们更好地对本教材做进一步改进。同时如果您在使用本教材的过程中遇到了什么问题，或者有什么好的建议，也请您来信告诉我们。

地址：北京市海淀区双清路学研大厦 A 座 602 室　计算机与信息分社营销室 收
邮编：100084　　电子邮件：jsjjc@tup.tsinghua.edu.cn
电话：010-62770175-4608/4409　　邮购电话：010-62786544

教材名称：信息安全体系结构

ISBN：978-7-302-17072-3

个人资料

姓名：＿＿＿＿＿＿　年龄：＿＿＿＿　所在院校/专业：＿＿＿＿＿＿＿

文化程度：＿＿＿＿＿＿　通信地址：＿＿＿＿＿＿＿＿＿＿＿＿

联系电话：＿＿＿＿＿＿　电子信箱：＿＿＿＿＿＿＿＿＿＿＿＿

您使用本书是作为：□指定教材 □选用教材 □辅导教材 □自学教材

您对本书封面设计的满意度：

□很满意 □满意 □一般 □不满意　改进建议＿＿＿＿＿＿＿＿＿＿

您对本书印刷质量的满意度：

□很满意 □满意 □一般 □不满意　改进建议＿＿＿＿＿＿＿＿＿＿

您对本书的总体满意度：

从语言质量角度看 □很满意 □满意 □一般 □不满意

从科技含量角度看 □很满意 □满意 □一般 □不满意

本书最令您满意的是：

□指导明确 □内容充实 □讲解详尽 □实例丰富

您认为本书在哪些地方应进行修改？（可附页）

＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿

＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿

您希望本书在哪些方面进行改进？（可附页）

＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿

＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿

电子教案支持

敬爱的教师：

为了配合本课程的教学需要，本教材配有配套的电子教案（素材），有需求的教师可以与我们联系，我们将向使用本教材进行教学的教师免费赠送电子教案（素材），希望有助于教学活动的开展。相关信息请拨打电话 010-62776969 或发送电子邮件至 jsjjc@tup.tsinghua.edu.cn 咨询，也可以到清华大学出版社主页（http://www.tup.com.cn 或 http://www.tup.tsinghua.edu.cn）上查询。